ICDS 2014

The Eighth International Conference on Digital Society

ISBN: 978-1-61208-324-7

March 23 - 27, 2014

Barcelona, Spain

ICDS 2014 Editors

Lasse Berntzen, Vestfold University College - Tønsberg, Norway
Åsa Smedberg, DSV, Stockholm University/KTH, Sweden
Andranik Tangian, Wirtschafts- und Sozialwissenschaftliches Institut - Düsseldorf |
Karlsruhe Institute of Technology, Germany

ICDS 2014

Foreword

The Eighth International Conference on Digital Society (ICDS 2014), held between March 23-27, 2014 in Barcelona, Spain, continued a series of international events covering a large spectrum of topics related to advanced networking, applications, and systems technologies in a digital society.

Nowadays, most of the economic activities and business models are driven by the unprecedented evolution of theories and technologies. These achievements are present everywhere in our society and it is only a question of user education and business models optimization towards a digital society.

Digital devices conquer from kitchen to space vessels most of the functionality commonly performed by human beings. Telecommunications, advanced computation, miniaturization, and high speed devices make tele-presence easy. Wireless and mobility allow ubiquitous systems to be developed. Progress in image processing and exchanging facilitate e-health and virtual doctor teams for patient surgeries.

Naturally, issues on how to monitor, control and manage these systems become crucial to guarantee user privacy and safety. Not only devices, but also special software features must be enforced and guaranteed in a digital society.

The variety of the systems and applications and the heterogeneous nature of the information and knowledge representation require special technologies to capture, manage, store, preserve, interpret and deliver the content and documents related to a particular target. In response to this challenge, Intrusion Prevention and Detection Systems have now grown in prominence to such an extent that they are now considered a vital component for any enterprise organisation serious about network defence. However, the numerous recorded attacks against high profile organizations is continuing evidence that many of these controls are not, at present, a panacea for dealing with the threats. Having themselves learnt the mechanisms employed by IPDS malicious parties are becoming particularly adept at evading them through inventive obfuscation techniques. These challenges need to be addressed using increasingly more innovative, creative and measurable IPDS mechanisms and methods.

Progress in cognitive science, knowledge acquisition, representation, and processing helped deal with imprecise, uncertain or incomplete information. Management of geographical and temporal information becomes a challenge, in terms of volume, speed, semantic, decision, and delivery.

Information technologies allow optimization in searching and interpreting data, yet special constraints imposed by the digital society require on-demand, ethics, and legal aspects, as well as user privacy and safety.

Nowadays, there is notable progress in designing and deploying information and organizational management systems, experts systems, tutoring systems, decision support systems, and in general, industrial systems.

The progress in difference domains, such as image processing, wireless communications, computer vision, cardiology, and information storage and management assure a virtual team to access online to the latest achievements.

Processing medical data benefits now from advanced techniques for color imaging, visualization of multi-dimensional projections, Internet imaging localization archiving and as well as from high resolution of medical devices. Collecting, storing, and handling patient data requires robust processing systems, safe communications and storage, and easy and authenticated online access.

National and cross-national governments' decisions for using the digital advances require e-Government activities on developmental trends, adoption, architecture, transformation, barrier removals, and global success factors. There are challenges for government efficiency in using these technologies such as e-Voting, eHealth record cards, citizen identity digital cards, citizen-centric services, social e-financing projects, and so on.

We take here the opportunity to warmly thank all the members of the ICDS 2014 Technical Program Committee, as well as the numerous reviewers. The creation of such a broad and high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and efforts to contribute to ICDS 2014. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations, and sponsors. We are grateful to the members of the ICDS 2014 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that ICDS 2014 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the area of digital society.

We are convinced that the participants found the event useful and communications very open. We hope that Barcelona, Spain, provided a pleasant environment during the conference and everyone saved some time to enjoy the charm of the city.

ICDS 2014 Chairs:

Lasse Berntzen, Vestfold University College - Tønsberg, Norway
Åsa Smedberg, DSV, Stockholm University/KTH, Sweden
Freimut Bodendorf, University of Erlangen, Germany
A.V. Senthil Kumar, Hindusthan College of Arts and Science, India
Charalampos Konstantopoulos, University of Piraeus, Greece
Andranik Tangian, Wirtschafts- und Sozialwissenschaftliches Institut - Düsseldorf | Karlsruhe Institute of Technology, Germany

ICDS 2014

COMMITTEE

ICDS Advisory Committee

Lasse Berntzen, Vestfold University College - Tønsberg, Norway
Åsa Smedberg, DSV, Stockholm University/KTH, Sweden
Freimut Bodendorf, University of Erlangen, Germany
A.V. Senthil Kumar, Hindusthan College of Arts and Science, India
Charalampos Konstantopoulos, University of Piraeus, Greece
Andranik Tangian, Wirtschafts- und Sozialwissenschaftliches Institut - Düsseldorf | Karlsruhe Institute of Technology, Germany

ICDS 2014 Technical Program Committee

Habtamu Abie, Norwegian Computing Center, Norway
Mir Abolfazl Mostafavi, Université Laval - Québec, Canada
Witold Abramowicz, The Poznan University of Economics, Poland
Gil Ad Ariely, Interdisciplinary Center Herzliya (IDC), Israel
Ali Ahmad Alawneh, Philadelphia University, Jordan
Adolfo Albaladejo Blázquez, Universidad de Alicante, Spain
Cristina Alcaraz, University of Malaga, Spain
Salvador Alcaraz Carrasco, Universidad Miguel Hernández, Spain
Eugenia Alexandropoulou, University of Macedonia, Greece
Shadi Aljawarneh, Isra University - Amman, Jordan
Giner Alor Hernández, Instituto Tecnológico de Orizaba-Veracruz, México
Aini Aman, Universiti Kebangsaan Malaysia, Malaysia
Pasquale Ardimento, University of Bari, Italy
Liliana Ardissono, Università di Torino, Italy
Charles K. Ayo, Covenant University, Nigeria
Gilbert Babin, HEC Montréal, Canada
Kambiz Badie, Research Institute for ICT, Iran
Ilija Basicevic, University of Novi Sad, Serbia
Farid E. Ben Amor, University of Southern California / DIRECTV, USA
Khalid Benali, LORIA -Université de Lorraine, France
Morad Benyoucef, University of Ottawa, Canada
Eleni Berki, University of Tampere, Finland
Lasse Berntzen, Vestfold University College - Tønsberg, Norway
Aljoša Jerman Blažič, SETCCE - Ljubljana, Slovenia
Marco Block-Berlitz, Hochschule für Technik und Wirtschaft Dresden, Germany
Freimut Bodendorf, University of Erlangen, Germany
Nicola Boffoli, University of Bari, Italy
Mahmoud Boufaida, Mentouri University of Constantine, Algeria
Danielle Boulanger, University of Lyon-Jean Moulin, France
Mahmoud Brahimi, University of Msila, Algeria
Diana Bri Molinero, Universitat Politècnica de València, Spain

Huong Ha, University of Newcastle, Singapore
Panos Hahamis, University of Westminster - London, UK
Gy R. Hashim, Universiti Teknologi Mara, Malaysia
Aboul Ella Hassanien, Cairo University, Egypt
Enrique Herrera-Viedma, University of Granada, Spain
Johann Höchtl, Donau-Universität Krems, Germany
Hana Horak, University of Zagreb, Croatia
Osman Ibrahim, British University in Egypt, Egypt
Rajesh Ingle, Pune University, India
Hany Abdelghaffar Ismail, German University in Cairo (GUC), Egypt
Marko Jäntti, University of Eastern Finland, Finland
Edward Jaser, Princess Sumaya University for Technology - Amman, Jordan
Maria João Simões, University of Beira Interior, Portugal
Janusz Kacprzyk, Polish Academy of Sciences - Warsaw, Poland
Sinchai Kamolphiwong, Prince of Songkla University - Songkhla, Thailand
Atsushi Kanai, Hosei University, Japan
Epaminondas Kapetanios, University of Westminster - London, UK
Kimmo Karhu, Aalto University, Finland
Sokratis Katsikas, University of Piraeus, Greece
Nermine Khalifa, Arab Academy for Science & Technology, Egypt
Spyros Kokolakis, University of the Aegean, Greece
Károly Kondorosi, Budapest University of Technology and Economics (BME), Hungary
Christian Kop, University of Klagenfurt, Austria
Ah-Lian Kor, Leeds Metropolitan University, UK
Andrew Kusiak, The University of Iowa, USA
Jaroslaw Kozlak, AGH University of Science and Technology - Krakow, Poland
Antti Lahtela, Unicta Ltd., Finland
Timo Lainema, Turku School of Economics, Finland
Wolfram Laaser, World Wide Education GmbH, Germany
John Lee, University of Edinburgh, UK
Igor Lemberski, Baltic International Academy, Latvia
Gen-Yih Liao, Chang Gung University, Taiwan
Diego Liberati, Politecnico di Milano, Italy
Ralf Lindner, Fraunhofer Institute for Systems and Innovation Research, Germany
Euripidis N. Loukis, University of the Aegean, Greece
Xudong Luo, Sun Yat-sen University, China
Antonio Marturano, Catholic University of the Sacred Heart, Italy
Peter Mikulecky, University of Hradec Králové, Czech Republic
Alok Mishra, Atilim University, Turkey
Harekrishna Misra, Institute of Rural Management Anand, India
John Morison, Queen's University - Belfast, UK
Paulo Moura Oliveira, INESC TEC - INESC Technology and Science (formerly INESC Porto)| UTAD University, Portugal
Debajyoti Mukhopadhyay, Maharashtra Institute of Technology, India
Darren Mundy, University of Hull, UK
Ahmad Nadali, Islamic Azad University, Iran
Syed Naqvi, CETIC, Belgium
Viorel Negru, West University of Timisoara, Romania

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Sensitivity of Information Disclosed in Amazon Reviews

Federica Fornaciari, C. Ranganathan, and V.N. Venkatakrishnan
University of Illinois at Chicago
Chicago, IL (USA)
fforna3@uic.edu, ranga@uic.edu, venkat@uic.edu

Abstract—**As online product reviews become ubiquitous, more individuals increasingly write and rely on them. In an effort to share their experiences and opinions about a product, do individuals share private and sensitive information online? This study addresses this critical issue by examining the extent of sensitive information disclosed in Amazon.com's product reviews. We crawled Amazon.com and gathered all online reviews posted for six products that pertained to weight loss, anti-aging, sex-related, fragrance, baby care and electronic goods. This resulted in 3,485 reviews, which were text-analyzed and mined using Linguistic Inquiry and Word Count (LIWC) analysis. Then, data processed through LIWC were further analyzed through descriptive statistics and discriminant analysis. We found that Amazon's reviewers disclose high levels of sensitive information in the following categories: family, humans, positive emotions, negative emotions, sadness, cognitive mechanisms, concerns related to work, achievements, leisure and money. Sensitive disclosure is also found to be a function of the type of reviewer and of the anonymization strategies adopted.**

Keywords-Privacy; Identity; Users-Generated Content; Sensitive Information; Natural Laguage Processing.

I. Introduction

With the wide spread of social network sites (SNSs) and the gained popularity of user-generated content, individuals increasingly share information online. The information posted online has various degrees of sensitivity and reveals different layers of one's personal life, identity [1], and personality traits [2]. Unfortunately, the features of online platforms open up the possibility of privacy infringements [3]. Despite the increased risks of losing control over personal information online, many still share several layers of the self, motivated by concerns that include desire of publicity [4], search for sociality [4], and narcissism [4]. The goal of this paper is to investigate patterns of self-disclosure in Amazon's reviews to further understand the levels of sensitivity of information shared by reviewers, and to provide implications related to end-user privacy concerns.

Amazon is a pioneer in incorporating customer reviews in e-commerce sites. Building on a history of improvements, the current review system in Amazon provides users with features such as ease-of-use and flexibility. For instance, users may decide to review products using their real name – and authorize Amazon to verify it using the credit cards information on their profile. Everyone, not just purchasers, has the possibility to review items. These vary from less personal products - as technology and electronics - to more personal ones - as baby products, weight loss, and anti-aging. Finally, Amazon provides the most active reviewers with different badges (e.g., Top Reviewer, Hall of Fame) to acknowledge their role within the Amazon's community. Reviews, at times, reveal detailed information about reviewers and/or about their family and friends. Perceived anonymity and trust in the community may encourage one to disclose different levels of sensitive information. And yet, deanonymization, privacy infringements, and loss of control over information may harm one's reputation and dignity, and generate psychological distress [5].

Exploring the extent of sensitive information shared in Amazon's reviews, this study pays attention to a number of factors, evaluating their role in encouraging reviewers to disclose information about the self and about others. In particular, this study measures and compares the levels of sensitive disclosure for reviewers based on their anonymization strategies (use of real name vs. nickname; location disclosure). Also, this study addresses the relationship between one's status within the Amazon's community - measured through the use of Amazon badges - and the sensitivity of information disclosed. In sum, the current research project contributes to understanding some of the factors that may encourage sensitive disclosure.

The organization of this paper is as follows. Section II discusses relevant literature. Section III outlines the problem investigated and the methodological approach. Section IV presents the findings. Sections V-VII explore and discuss findings and limitations of the current study.

II. Literature Background

A. Risks and Opportunities of Self-disclosure Online

Despite initial dystopian views, most research shows that individuals who interact through social media are exposed to both risks and opportunities. In fact, research suggests that SNSs may facilitate ties creation and maintenance, online community formation [6], [7], identity development [4], psychological reassurance, and self-expression [8]. Self-disclosure online, though, also entails risks of privacy infringements and identity theft [9], [10], commercial use of personal information [11], damages to reputation [5] stalking, reinforcing stereotypes and discrimination [12].

Clearly, self-disclosure online is an increasingly popular activity as users "share their ideas, interests, emotions, experiences, and knowledge with other" on the Web [13, p. 234]. Research has explored the motivations that may encourage one to share personal information online. Among the perceived benefits of disclosure scholars identify four main areas: cognitive needs (as information seeking), affective needs (as entertainment), social integrative needs (as forming communities), and personal integrative needs (as identity formation) [14].

Social media provide new stages for sociality [3]. Research shows that social media are designed for sharing and connecting rather than for protecting privacy [8]. As a consequence, self-disclosure online may challenge one's ability to control personal information and to manage private and public boundaries [10]. Self-presentation online is crafted to show different angles of the self to different audiences. One may connect to distinct spheres of sociality showing different facets of one's identity depending on one's envisioned, desired or perceived audience. In such a process of disclosure, one may consider surveillance, data-mining, and behavioral marketing as remote possibilities or acceptable tradeoffs to enjoy the benefits of socialization and online community that may stem from disclosure [8]. Unfortunately though, managing levels of accessibility for different viewers is challenging and time-consuming, and ability to do so is often a function of internet literacy [3].

Research investigated the dynamics of social media reframing old questions and introducing new ones. However, as of yet, there are not studies that investigate self-disclosure in consumers' reviews sites. The current study addresses this gap in the attempt to identify and evaluate the disclosure of sensitive information (and the possible implications for privacy) in online platforms supposedly dedicated to e-commerce.

B. *Sensitivity of Information*

Research thoroughly explored the relationship between sensitivity of information and willingness to disclose often showing a negative correlation between the two [15]. However, most research focused on the sensitivity of information explicitly requested or required by a site. The current study is novel in its attempt to develop a method to evaluate the sensitivity of information disclosed in the unstructured texts of consumers' reviews that do no necessarily encourage sensitive disclosure.

Personal information may have different levels of sensitivity. Research often relates information sensitivity to its level of intimacy. Previous research adopted a number of strategies to measure depth and breadth of self-disclosure in consumers' reviews and online forums [16].

The main contribution of this paper is to measure the extent of self-disclosure on Amazon reviews and analyze on its privacy implications. Our approach is a quantitative one that aims to measuring the extent of self-disclosure. The main assumption of the current study is that language may be used as a valuable indicator of the sensitivity of information disclosed. Such an assumption draws from abundant research published in cognitive psychology that suggests that the words may be reflective of one's social relationships, personality, social behavior, and cognitive style. The use of language is also a meaningful indicator to measure the disclosure of positive or negative emotions and other psychological processes [13], [17], as well as personality traits [2]. Words used may also reveal a variety of sensitive information [18], [19], [20], [21].

Our methodology involves measuring the sensitivity of information disclosed using the Linguistic Inquiry and Word Count (LIWC) software. LIWC has built-in dictionaries used to count words and separate them in psychologically meaningful categories. LIWC allows to process large samples of text thus providing valuable quantitative insight. Thus, LIWC provides a unique analytic approach that allows studying the granularity of information disclosed. Over decades of use, LIWC has been tested for validity and reliability of results, and successfully implemented to analyze text in a large variety of categories [17], [18].

For the scope of this study, the degree of sensitivity of information disclosed was measured using the framework adopted in Tausczik and Pennebaker's work [17] and implemented through the software LIWC. In particular, this study used LIWC to measure the following: social processes (family, friends, humans), affective processes (swear, positive emotion, negative emotion, anxiety, anger, sadness, cognitive mechanisms), biological processes (health, sexual), and personal concerns (work, achievements, leisure, home, money, religion, death) [17], [18].

Alternative scalable methods to study sensitive information in large portions of text include opinion mining, sentiment analysis, and other forms of natural language processing. These methods allow one to investigate point of view and subjectivity as they emerge from textual analysis [22]. For example, opinion and sentiment analysis have been successfully implemented for fake reviews detection in Amazon [23] or to mine and classify opinions and emotions from reviews in the blogosphere [13]. Alternatively, natural language processing has enabled the study of personality traits in SNSs [2]. Even though opinion and sentiment mining are very powerful methodological approaches, they tend to focus on solving opinion-oriented classification problems. As a consequence, they were not considered suitable for the scope of this study.

C. *Research Questions*

In particular, data were collected to address the following research questions:

RQ1 - To what extent do Amazon's reviewers reveal sensitive information when reviewing a product?

RQ2 – Is there a relationship between the disclosure of sensitive information and the use of a real name?

RQ3 – Is there a relationship between the disclosure of sensitive information and the disclosure of one's location?

RQ4 – Is there a relationship between type of reviewer and sensitivity of information disclosed?

III. METHOD

A. *Types of Products*

Amazon includes a large number of products whose nature may encourage different degrees of disclosure. For the current research, we selected six products across the spectrum in the attempt to implement a study that would be doable yet comprehensive, exploring a breadth of products that may prime individuals to disclose different kinds of sensitive information. The items selected pertained to the following categories: sex-related, weight loss, anti-aging, fragrance, baby care, and electronic.

B. *Variables and Data Collection*

Amazon reviews are public. This facilitated the data collection that was operated through a crawler launched in the Amazon website in November 25th, 2012. The data collection process generated 3,485 .txt files of review for six different products. The unit of analysis was the single review. Each file included the text of the review as well as the following variables: real name (y/n), top reviewer (y/n), hall of fame reviewer (y/n), vine voice (y/n), length of review, location (y/n), number of stars (1-5), and number of reviews posted by the reviewer.

Some of these variables are identified through badges that Amazon awards to its reviewers. In particular, the badges Top Reviewer and Hall of Fame identify, respectively, reviewers who provided the most helpful contributions recently and longitudinally. The badge Vine Voice is provided to reviewers who received a free product for review. Finally, for the purpose of the study, "location" was turned into a yes/no categorical variable to distinguish between those who disclosed a "realistic location" (that included both city and state) from those who did not disclose their location or that provided vague or unrealistic information (e.g., state only, country only, or phantasy names).

The texts of the reviews were processed through the software LIWC to measure multiple variables that could be used as indicator of sensitive information. In particular, based on existing literature, the current study considered the "level of sensitivity" of information as a multidimensional variable. LIWC allowed measuring the percentage of words belong in each of the following categories: social processes (family, friend, humans); affective processes (swear, positive emotion, negative emotion, anxiety, anger, sadness, cognitive mechanisms); biological processes (health, sexual); and personal concerns (work, achievements, leisure, home, money, religion, death). Afterwards, we merged the six result files created through LIWC to generate a comprehensive spreadsheet that could be inputted in SPSS for statistical analysis.

IV. DATA ANALYSIS

To describe our sample we run descriptive statistics for the whole 3,485 reviews. Descriptive statistics included frequencies for categorical variables (real name, top reviewer, hall of fame reviewer, vine voice, and location). They included means, standard deviations, and range for continuous variables (length of review, and number of reviews posted by the reviewer).

Our sample included a larger number of reviewers who did not disclose their real name (72.4%), or their location (72.4%). Most did not belong in the Hall of Fame (99.8%), in the Top Reviewer (98.8%) or in the Vine Voice (96.4%). The typical reviewer in our sample published 30 reviews (SD = 216; range = 5675), whose average length was of 97 words (SD = 107.64; range = 2080). In addition, most reviews were positive. In particular in a scale from 1 (worst) to 5 (best) the average number of stars was M = 4.26, SD = 1.23.

A. *RQ1 - To what extent do Amazon's reviewers expose sensitive information when reviewing a product?*

To answer the first research question, we measured the percentages of use of words per category of sensitive information in our sample. Then, we compared these results with the average level of information disclosed derived from a study conducted by Pennebaker and colleagues [17]. The latter study is the outcome of a collection and analysis of words used across a variety of settings including: emotional writing, control writing, science articles, blogs, novels, and talking (aggregated sample, N = 721,726).

From the comparison, Amazon reviewers use significantly more words belonging in the following categories: family (overall mean of use = .48%), humans (.78%), positive emotions (5.12%), negative emotions (1.7%), sadness (.48%), cognitive mechanisms (17.03%), and concerns related to work (2.71%), achievements (3.31%), leisure (1.31%), and money (1.66%). Significance was measured at the 95% confidence level.

B. *RQ2 - Is there a relationship between the disclosure of sensitive information and the use of a real name?*

To address the second research question we analyzed the whole sample comparing the disclosure of sensitive information for those who used a real name badge against those who did not. As we ware exploring the relationship between a categorical variable (real name badge) and a multidimensional continuous variable (level of sensitivity), we measured the strength of the relationship using a *discriminant analysis* with a 95% level of confidence.

The discriminant analysis highlighted some significant difference in the word use between the real name group and the non-real name group. In particular, reviewers who disclosed their real name were significantly more likely to use words in the following categories: sadness (Wilk's Lambda = .996, F = 14.09), health (Wilk's Lambda = .994, F=20.60), and concerns related to achievements (Wilk's Lambda=.995, F=16.79). The real name group was less significantly likely to discuss leisure-related concerns (Wilk's Lambda = .985, F = 51.32). Unfortunately, our sample included a larger number of non-real name reviewers (non-real name N = 2524; real name N = 961). As a consequence, the differences found may be affected by the differences in the size of the groups compared.

Finally, we calculated the level of sensitive information aggregating the frequencies of words use for all the categories analyzed. Such an aggregated value was then used to conduct a second *discriminant analysis* at the 95% level of confidence. Interestingly, such an analysis revealed a significant difference (Wilk's Lambda = .999; sig. = .023) showing that, overall, reviewers who used their real names disclosed higher levels of sensitive information.

In sum, individuals who used real names tended to disclose more information involving sadness, health processes and concerns related to personal achievements. They were less likely to discuss leisure-related concerns.

C. RQ3 - Is there a relationship between the disclosure of sensitive information and the disclosure of one's location?

To answer the third research question we compared the disclosure of sensitive information for those who provided their location against those who did not (or disclosed a vague or unrealistic location). To measure the strength of such a relationship, we used *discriminant analysis* with a 95% level of confidence to test each category of sensitive information. Afterwards, we run a second *discriminant analysis*, still at the 95%, to test the aggregated disclosure of sensitive information.

From the first discriminant analysis, we found significant differences in information disclosure between reviewers who revealed their real location and those who did not. In particular, those who disclosed their location were significantly more likely to use words in the following categories: sadness (Wilk's Lambda = .997, F = 11.48), health (Wilk's Lambda = .994, F = 20.75), achievements (Wilk's Lambda = .998, F = 6.80), and religion (Wilk's Lambda = .997, F = 10.43). They were significantly less likely to use words that belong in the following categories: positive emotions (Wilk's Lambda = .998, F = 7.01), sexual concerns (Wilk's Lambda = .998, F = 8.24), and leisure (Wilk's Lambda = .987, F = 47.40). Similarly to RQ2, reviewers who disclosed their location (N = 962) were much less than those who did not (N = 2,523). The second *discriminant analysis* showed that those who disclosed their location were slightly more likely to share sensitive information. Yet, such a difference was not found to be significant.

In sum, and consistently with the findings related to RQ2, individuals who disclosed their location tended to use more words related to sadness, they discussed more health processes, and were more likely to tackle concerns related to personal achievements.

D. RQ4 - Is there a relationship between type of reviewer and sensitivity of information disclosed?

To address the fourth research question we run a number of *discriminant analyses* at the 95% level of confidence to evaluate the relationship between each of the categorical variables related to the "type of reviewer" (Hall of Fame, Top, Vine Voice) and the multilevel continuous variable "level of sensitivity." As a result, some statistically significant differences were found.

In particular, Hall of Fame reviewers were significantly less likely to disclose affective processes (sig = .048; F = 3.903). Vine Voice reviewers were significantly less likely to use words belonging in the following categories: family (sig. = .007; F = 7.19), friends (sig. = .031; F = 4.68), humans (sig. = .001; F = 10.2), affective processes (sig. = .000; F = 26.7), positive emotions (sig. = .000; F = 12.58), negative emotions (sig. = .000; F = 12.33), anger (sig. = .002; F = 9.6), sadness (sig. = .031; F = 4.67), cognitive mechanisms (sig. = .000; F = 22.7), leisure (sig. = .000; F = 21.78), home (sig. = .048; F = 3.9), and money (sig. = .000; F = 20.43). Top reviewers were significantly less likely to use words belonging in the following categories: affective processes (sig. = .004; F = 8.22), positive emotions (sig. = .043; F = 4.1), leisure (sig. = .042; F = 4.1), and money (sig. = .031; F = 4.66). Verified Purchase reviewers were more likely to use words in the following categories: swear (sig. = .019; F = 5.5), affective processes (sig. = .000; F = 18.93), positive emotions (sig. = .000 F = 16.04), work (sig. = .000; F = 13.1), achievement (sig. = .012; F = 6.27), and leisure (sig. = .000; F = 52.24). They were less likely to use words belonging in the categories that follow: humans (sig. = .014; F = 6.06), and health (sig. = .004; F = 8.5).

Additionally, we run discriminant analysis at the 95% level of confidence to gauge the relationship between type of reviewers and aggregated level of sensitive information disclosed. Such an analysis revealed significant differences in the disclosure of sensitive information. In particular, the groups more likely to engage in such a disclosure were the following: non-Hall of Fame reviewers (Wilk's Lambda = .997; sig. = .002); non-Top reviewers (Wilk's Lambda = .996; sig. = .000); non-Voice Vine, (Wilk's Lambda = .993; sig. = .000).

Unfortunately, the sample analyzed included importantly larger number of "regular reviewers" (non belonging in the categories Hall of Fame, Top, or Vine Voice). Such a distribution may likely reflect the general composition of the Amazon community – where most reviewers are occasional and non-professional - yet the differences found in our analysis are likely affected by the differences in the size of the groups compared.

In sum, regular reviewers (as opposed to reviewers who are awarded the special badges identified in this study) were often more likely to disclose sensitive information. They consistently tended to share higher level of personal information belonging in many categories, perhaps as a way to increase their personal participation in the Amazon community. These results may be consistent with common sense expectations. Yet, further research is necessary to further explore them, as the sample used in the current study included a limited number of non-regular reviewers (e.g., Top, Hall of Fame).

V. DISCUSSION

As it emerged from our analysis, Amazon reviewers in the sample collected tend to reveal higher level of sensitive information, compared to the average [17], in the following categories: family, humans, affect, positive emotions, negative emotions, sadness, cognitive mechanisms, and concerns related to work, achievements, leisure and money. Such a finding may suggest that people who post reviews online do so to actively participate in the Amazon community. Perhaps, they feel to be part of a trusted social circle within which one feels relatively safe in the disclosure of sensitive information about the self and the others – maybe without considering that Amazon reviews are public. These reviewers, in fact, do not seem to post reviews for the gratification of receiving specific badges (otherwise they would be more active reviewers). And yet, they share high levels of sensitive information - levels that increase for those who also disclose their real offline identity (name and location). Trust in the perceived community may be an important component of the equation. These findings seem to suggest that many experience Amazon as a venue built around people who show their humanity, their social connection, their affective processes, their emotions, and their concerns. Current findings also suggest that many consider Amazon as a platform for building community and sharing information about one's social circles. Doing so, users partly "reinvent Amazon" by mingling the affordances of online retailing websites with those of SNSs [6]. Amazon, similarly to most social media, becomes a platform structured around individuals, where users may become the center of personal communities that share interests and life experiences.

Consistent with research conducted to understand participation in SNSs, this study may suggest that a large component of Amazon reviewers behave as active members of a community and use the website as a platform to perform their identity. Previous research suggests that those who are active SNSs users tend to have lower privacy concerns [24]. Such a consideration may apply to the current study as well. Admittedly, though, the data we collected and analyzed are not sufficient to claim that individuals who post product reviews on Amazon are less concerned about their privacy. However, our findings show that individuals who decide to post reviews online are likely to talk about their personal experiences - as well as about their social relationships – often disclosing high levels of sensitive information. And levels of disclosure increase for non-anonymous reviewers.

As detailed in Section II, research shows that need of social capital and desire of community building are strong factors motivating individuals to disclose information. Similarly, high levels of self-disclosure in Amazon may be motivated by the desire to develop and maintain online community. Amazon makes it easy for its users to post and read reviews and comments, perhaps presenting itself as a network that fosters sociality and publicity, and thereby encouraging users to disclose rather than withhold information. Similarly to what research has pointed out for SNSs [9], Amazon's network seem to have a large utility for its users who can develop sense of belonging and participation. Importantly, such a potential may implicitly encourage users to disclose - thereby also increasing the commercial value of Amazon.

The importance of Amazon for community building begins to emerge from the data addressing the first three research questions. In particular, individuals who disclose their identity in Amazon (real name and/or location) tend to disclose more information about their social processes, their sadness, their biological and health processes and their concerns related to personal achievements. Findings related to RQ2 and RQ3 reveal fairly similar tendencies, suggesting that individuals who disclose more information about their offline identity (real name and location) are also those who appear to need social support. In fact, they disclose personal concerns as to reveal their needs and their weaknesses (e.g., sadness and concerns). As research suggests, individuals who seek social capital are often willing to accept privacy risks [12].

Finally, data analyzed to answer the fourth research question emphasize that "normal reviewers" consistently tend to share higher levels of sensitive information thus increasing their personal participation in the Amazon community. Unfortunately, this finding was significantly limited by the fact that our sample included few reviewers belonging in the categories Top, Hall of Fame and Vine Voice. To address such a limitation, a future study could be conducted from a users-centered perspective (using the reviewer as unit of analysis - instead of the review as we did in the current study - and collecting reviews based on the use of badge). A comparison of equally sized groups of reviewers would allow a better assessment of these findings.

VI. Limitations

Even though this study provided a number of contributions to the understanding of disclosure in online reviews, its scope had some limitations. Needless to say, Amazon commercializes thousands of products that belong in a wide variety of categories. Despite the attempt to select a number of products that would provide multiple perspectives to render the variety of patterns of self-disclosure in Amazon, the sample was limited to six products and, likely, provided a partial representation of the population analyzed. Thus, results may not be generalized to the entirety of Amazon's reviews, or to other communities of consumer's reviews. Despite such a limitation though, we believe that the current study provided a valuable contribute to research tackling online disclosure and related privacy risks. The use of LIWC and its ability to capture the granularity of information, particularly contributed to this outcome.

Also, some could argue that the LIWC software limits its evaluation of sensitive information to the use of words, taking them outside of their context of delivery. As a consequence, one may suggest that LIWC fails to capture the nuances of language, and label words as belonging in a category they do not really belong in. Even though such a critique may provide some fundamental insight that one need to take into consideration when analyzing text, it is normally assumed that the analysis of large samples of text (ours included 3,845 reviews) would control for such a risk.

VII. Conclusions

In this paper, we examined the extent of sensitive information disclosed in Amazon.com's product reviews. This was done by crawling Amazon's pages and gathering all online reviews posted for six products that pertained to weight loss, anti-aging, sex-related, fragrance, baby care and electronic goods. This resulted in 3,485 reviews, which were text-analyzed and mined using LIWC analysis. We further analyzed the results of the text-analysis through descriptive statistics and discriminant analysis. We found that Amazon's reviewers disclose higher levels of sensitive information in the following categories: family, humans, positive emotions, negative emotions, sadness, cognitive mechanisms, concerns related to work, achievements, leisure and money. In addition, occasional and non-professional reviewers provided higher level of sensitive information, perhaps as a way to increase their participation in the Amazon community.

The conclusions for our study raises several open questions: first, whether it would be possible, by using methods similar to ours, to provide usable warning indicators that inform end-users when they input privacy sensitive reviews. A more ambitious (but perhaps more usable) system would also provide deanonymizing suggestions in case the system finds certain reviews to be sensitive. Continuing to retain the high quality of reviews similar to those found in Amazon, while providing deanonymizing suggestions would be a challenge to current socio-technical systems.

VIII. Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. DGE-1069311.

IX. References

[1] D. G. Weckowski and J. Małyszko, “On information exchange for virtual identities: survey and proposal,” *ICSD 2013 - The Seventh International Conference on Digital Society,* March, 2013, pp. 59-64.

[2] F. Celli, “Unsupervised personality recognition for social network sites,” *ICSD 2012 - The Sixth International Conference on Digital Society,* March, 2012, pp. 59-62.

[3] A. Marwick and D. Boyd, “I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience,” *New Media & Society,13(1),* pp. 114-133, 2011.

[4] A. L., Mendelson and Z. Papacharissi, “Look At Us: Collective Narcissism in College Student Facebook Photo Galleries,” in *A Networked Self: Identity, Community, and Culture on Social Network Sites*, Z. Papacharissi, Ed. New York: Routledge, 2011.

[5] D. J. Solove, “The Future of Reputation: Gossip, Rumor, and Privacy on the Internet,” Yale University Press, 2007.

[6] D. Boyd and N. Ellison, “Social Network Sites: Definition, History, and Scholarship,” *Journal of Computer-Mediated Communication, 13*, pp. 210-230, 2008.

[7] M. Forestier, J. Velcin, D. A. Zighed, “Analyzing social roles using enriched social network on on-line sub-communities,” *ICSD 2012 - The Sixth International Conference on Digital Society,* March, 2012, pp. 59-62.

[8] J. Jarvis, “Public Parts. How Sharing in the Digital Age Improves the Way We Work and Live’” New York: Simon & Schuster, 2011.

[9] A. Acquisti and R. Gross, “Imagined communities: Awareness, information sharing, and privacy on the Facebook,” in *Proceedings of 6th Workshop on Privacy Enhancing Technologies*, P. Golle & G. Danezis, Eds. Cambridge, U.K.: Robinson College, 2006.

[10] H. Nissenbaum, “Privacy in Context. Technology, Policy, and the Integrity of Social Life,” Stanford: Stanford Law Books, 2010.

[11] A. Odlyzko, “Privacy and the clandestine evolution of e-commerce,” *ICEC 2007 - Proceedings of the ninth international conference on Electronic commerce*. New York, NY, USA: ACM, August, 2007, pp. 3-6.

[12] N. Ellison, C. Lampe, C. Steinfield, and J. Vitak, “With a Little Help From My Friends. How Social Network Sites Affect Social Capital Processes,” in *A Networked Self: Identity, Community, and Culture on Social Network Sites*, In Z. Papacharissi, Ed. New York : Routledge, 2011.

[13] A. Baloglu and M. S. Aktas, “An Automated Framework for Mining Reviews from Blogosphere,” *International Journal of Advances in Internet Technology, 3(3&4),* pp. 234-244, 2010.

[14] L. Leung. “User-generated content on the internet: an examination of gratifications, civic engagement and psychological empowerment,” *New Media & Society, 11,* pp. 1327–1347, 2009.

[15] D. L. Mothersbaugh, W. K. Foxx, S. E. Beatty, and S. Wang, “Disclosure antecedents in an online service context: The role of sensitivity of information,” *Journal of Service Research, 15(1),* pp. 76-98, 2012.

[16] Y. Moon, “Intimate exchanges: Using computers to elicit self ‐ disclosure from consumers,” *Journal of Consumer Research, 26(4),* pp. 323-339, 2000.

[17] J. W. Pennebaker, R. J. Booth, and M. E. Francis, “Operator’s Manual. Linguistic Inquiry and Word Count,” 2007.

[18] Y. R. Tausczik and J.W. Pennebaker, “The psychological meaning of words: LIWC and computerized text analysis methods,” *Journal of Language and Social Psychology, 29(1),* pp. 24–54, 2010.

[19] G. W. Alpers, et al., “Evaluation of computerized text analysis in an Internet breast cancer support group,” *Computers in Human Behavior, 21*, pp. 361-376, 2005.

[20] D. J. Houghton and A. N. Joinson, “Linguistic markers of secrets and sensitive self-disclosure in Twitter,” *45th Hawaii International Conference on System Science (HICSS)*. IEEE, January, 2012, pp. 3480-3489.

[21] J. M. Smyth, “Written emotional expression: Effect sizes, outcome types, and moderating variables,” *Journal of consulting and clinical psychology, 66(1),* pp. 174-184, 1998.

[22] B. Liu, “Sentiment analysis and opinion mining,” *Synthesis Lectures on Human Language Technologies, 5(1),* 2012.

[23] B. Liu, “Sentiment analysis and subjectivity,” *Handbook of Natural Language Processing*, pp. 627–666, 2010.

[24] J. Fogel and E. Nehmad, “Internet social network communities: Risk taking, trust, and privacy concerns,” *Computers in Human Behavior, 25*, pp. 153-160, 2009.

A Secure and Flexible Server-Based Mobile eID and e-Signature Solution

Christof Rath, Simon Roth, Manuel Schallar and Thomas Zefferer
Institute for Applied Information Processing and Communications
Graz University of Technology
Graz, Austria
Email: {first name}.{last name}@iaik.tugraz.at

***Abstract*—In our digital society, e-government, e-commerce, and e-business are increasingly gaining importance. Many services of these domains rely on reliable user authentication and electronic signatures. For many years, smart cards have been the technology of choice to implement eID and e-signature solutions. Recently, mobile eID and e-signature solutions have emerged as an attractive alternative, as they provide better usability compared to smart card based approaches while maintaining the same level of security. Unfortunately, most current mobile eID and e-signature solutions are tailored to the needs of specific application scenarios and hence cannot easily be applied to and used for other use cases. This prevents a broad use of mobile eID and e-signature solutions and leads to a situation, in which many services still rely on smart card based approaches with poor usability or even insecure password-based solutions for user authentication. To overcome this issue, we propose an improved mobile eID and e-signature solution. In contrast to existing comparable solutions, the proposed solution has been designed such that compatibility with arbitrary use cases is guaranteed. This way, its integration into arbitrary services and applications is facilitated. The feasibility and applicability of the proposed solution has been successfully evaluated by means of a concrete implementation. This implementation demonstrates that the proposed solution provides a secure and usable alternative to existing eID and e-signature solutions and has the potential to improve the security of various e-government services and applications from private-sector domains.**

Keywords*—*eGovernment; eID; electronic identity; electronic signature; identity management; mobile security.

I. Introduction

With the rise of the digital society, remote identification of users has become an increasing challenge as a growing number of services have been moved to the Internet. This applies to public-sector applications (e-government) as well as to private-sector applications (e-commerce, e-business). Remote identification is usually achieved by means of a unique electronic ID (eID) assigned to the user. An eID can for instance be a unique number, user name, or e-mail address. During authentication, the claimed identity (eID) is proven by the user. Reliance on secret passwords for authentication purposes is still the most popular and most frequently used authentication approach for online services. However, password-based authentication schemes have turned out to be insecure due to their vulnerability against phishing attacks and their poor usability, which often leads to the use of weak passwords that are easy to guess [1] [2].

Transactional online services from the e-government domain and related fields of application typically require reliable remote identification and authentication of users. Given the obvious drawbacks of password-based eID and authentication schemes in terms of security, two-factor authentication schemes have been developed for applications with high security requirements such as transactional e-government services. Current two-factor authentication schemes typically comprise the authentication factors *possession* and *knowledge*.

Popular examples of two-factor authentication schemes are smart card based solutions. During the authentication process, the user proves to be in *possession* of the eID token (i.e., the smart card) and proves *knowledge* of a secret PIN that is specific to this eID token and that protects access to the token and to eID data stored on it. In most cases, smart cards additionally enable users to create electronic signatures (e-signatures). For this purpose, the smart card additionally stores a secret signing key and features hardware-based signature-creation capabilities. Access to the signing key and to the smart card's signature-creation functionality is again protected by means of two-factor authentication.

Smart cards are an ideal technological choice to combine the concepts of eID and e-signature, as they are capable to implement both eID and e-signature functionality. Thus, they are frequently used in security-critical fields of application such as e-business, e-banking, or e-government. For instance, various transactional e-government services that have been launched in Europe during the past years require users to authenticate remotely with a personalized smart card and to complete online transactions by applying an electronic signature with the same card [3]. Unfortunately, smart card based solutions usually lack an appropriate level of usability, as they require users to obtain, install, and use an appropriate card-reading device [4].

Powered by the recent emergence of mobile communication technologies and motivated by the low user acceptance of smart card based eID and e-signature solutions, several mobile eID and e-signature solutions have been developed during the past years [5]. These solutions render the use of smart cards unnecessary, as they cover the authentication factor *possession* by means of the user's mobile phone. This way, mobile eID and e-signature solutions have the potential to significantly improve usability while maintaining the same level of security as smart card based solutions.

Due to their improved usability compared to smart card based authentication schemes [4], mobile eID and e-signature

ISBN: 978-1-61208-324-7

solutions are in principle also suitable for use cases with lower security requirements. Unfortunately, existing mobile eID and e-signature solutions are usually tailored to the requirements of specific use cases and fields of application. This applies to most mobile eID and e-signature solutions that have been introduced and launched worldwide during the past years. Due to their limitation to specific use cases, these solutions can hardly be used in different fields of application. This leads to a situation, in which most applications cannot benefit from the enhanced security and usability of existing mobile eID and e-signature solutions.

To overcome this problem, we propose a modular and flexible concept for mobile eID and e-signature solutions. The main idea behind the design of the proposed concept was to achieve a flexible solution and to maintain its compatibility to different use cases and application scenarios. Details of the proposed concept are presented in this paper. In Section II, we start with a brief survey of existing mobile eID and e-signature solutions and discuss their strengths and limitations. We then derive requirements of a mobile eID and e-signature solution that is applicable in arbitrary application scenarios in Section III. In Section IV, we introduce a technology-agnostic architecture for a mobile eID and e-signature solution that meets all predefined requirements. Based on the proposed architecture, we model three technology-agnostic processes that cover the functionality of the proposed solution in Section V. The practical applicability and feasibility of the proposed solution is assessed in Section VI by means of a concrete implementation. Finally, conclusions are drawn in Section VII.

II. Related Work

The reliable remote identification and authentication of users by means of two-factor based approaches has been a topic of scientific interest for several years. Two-factor based authentication schemes based on smart cards have been introduced in several security-sensitive fields of application during the past decades. Especially in Europe, various countries, such as Austria [6], Estonia [7], Belgium [8], or Spain [9] have issued personalized smart cards to their citizens in order to reliably identify and authenticate them during transactional e-government procedures [3]. In various fields of application, smart cards also enable users to create electronic signatures during online procedures. For instance, electronic signatures are of special importance in Europe, where electronic signatures can be legally equivalent to handwritten signatures according to the EU Directive 1999/93/EC [10].

While smart cards work fine from a functional point of view, their usability is usually rather poor due to the need for a card-reading device to physically connect the smart card to the user's computer. The need for additional drivers and software to communicate with the smart card and to integrate its functionality into security-critical applications also decreases the usability of smart-card technology in general and of smart card based eID and e-signature solutions in particular [4].

To overcome given usability issues of smart card based solutions, several mobile two-factor based eID and e-signature solutions have been developed during the past years. Surveys of mobile eID and e-signature solutions have for instance been provided by Ruiz-Martinez et al. [5] and Pisko [11]. All these solutions have in common that the factor *possession* is not covered by a smart card but by the user's mobile phone. All mobile eID and e-signature solutions that comply with demanding legal requirements, such as those defined by the EU Signature Directive include some kind of secure hardware element, which is able to securely store eID data and to carry out cryptographic operations. Depending on the realization and location of this secure hardware element, mobile eID and e-signature solutions can be basically divided into the following two categories:

- **SIM-based solutions:** Solutions belonging to this category make use of the mobile phone's SIM (subscriber identity module) to securely store eID data and to carry out cryptographic operations. In most cases, the use of a special SIM is required, as off-the-shelf SIMs do not feature the required cryptographic operations such as the creation of electronic signatures. Access to eID data stored on the SIM and to cryptographic functionality provided by the SIM is typically protected by a secret PIN that is only known to the legitimate user. This PIN covers the factor *knowledge* of the two-factor based authentication scheme.
- **Server-based solutions:** Server-based mobile eID and e-signature solutions implement the secure hardware element centrally e.g., in a hardware security module (HSM). Such a solution has been proposed by Orthacker et al. [12]. The user's mobile phone does neither implement cryptographic functionality, nor store eID data. However, the mobile phone is an integral component of the authentication process that is mandatory in order to gain access to centrally stored eID data and to carry out electronic signatures. In most cases, the mobile phone acts as receiver for one-time passwords (OTP), which have then to be sent by the user to the central HSM in order to prove *possession* of the mobile phone and to complete the authentication process.

For both above-mentioned categories, concrete mobile eID and e-signature solutions have been developed and rolled-out on a large scale. For instance, SIM-based mobile eID and e-signature solutions have been set into productive operation in Estonia [13] and Norway [14]. A server-based mobile eID and e-signature solution has been in productive operation in Austria since 2009 [15]. Most existing solutions are tailored to a specific legal framework (e.g., national laws) or to a certain identity system (e.g., to a specific national eID system). For instance, the Austrian mobile eID and e-signature solution has been purpose-built for the Austrian official eID infrastructure and bases on data structures, protocols, and registers that are specific to the Austrian use case. Deploying this solution in other countries would require major adaptations and cause additional costs. Similar limitations apply to most mobile eID and e-signature solutions that have been set into productive operation so far. This renders an application of these solutions in different fields of application difficult and expensive, and prevents that all applications can benefit from the improved security and usability of mobile eID and e-signature solutions.

III. Requirements

The conducted survey on existing mobile eID and e-signature solutions has identified a lack of dynamically adaptable solutions that can easily be applied to arbitrary use cases. To remove this issue, we propose a mobile eID and e-signature solution that can easily be used in arbitrary application scenarios. We have designed the proposed solution, which will be introduced in Sections IV and V in detail, according to a set of requirements. These requirements have been extracted from an analysis of existing solutions and from published evaluations of these solutions such as [4]. The derived requirements (R1-R5) are discussed in the following in more detail.

- **R1:** **Flexibility regarding external components:** Mobile eID and e-signature solutions typically rely on external parties and components. Common examples for such components are certification authorities (CA), which bind a user's identity to her signing key, or identity databases (e.g., official person registers or company databases), which are required to derive eIDs for users. A generic mobile eID and e-signature solution must not be limited to certain external components but provide flexible means to integrate different external components (e.g., different CAs).
- **R2:** **Avoidance of token roll-outs:** Long-term experience with smart card based solutions has shown that the roll-out of eID and e-signature tokens (e.g., smart cards, SIMs) causes additional (financial) effort and hence reduces user acceptance. Avoidance of necessary roll-outs of such tokens is hence a key requirement for usable mobile eID and e-signature solutions.
- **R3:** **Usability:** The often disappointing user acceptance of smart card based solutions shows that usability is an important success factor of eID and e-signature solutions. For mobile eID and e-signature solutions, the following aspects need to be considered in particular in order to achieve an appropriate level of usability:
  - **R3a:** **Avoidance of installations:** Usable solutions must not require the user to obtain, install, and maintain additional hardware or software, as this causes additional effort.
  - **R3b:** **Platform and device independence:** Usable solutions must not be restricted to certain computing platforms, operating systems, or end-user devices, as users want to access services everywhere and at any time irrespective of their current execution environment.
  - **R3c:** **Location independence:** Usable mobile eID and e-signature solutions must not be bound to a certain mobile network but must also be accessible when roaming in foreign networks.
- **R4:** **Security:** Security is an important requirement, as mobile eID and e-signature solutions are mainly applied in security-sensitive fields of application such as e-government or e-commerce. Hence, mobile solutions must assure the same level of security as other two-factor based eID and e-signature solutions and must be able to comply with given legal requirements such as the EU Signature Directive.
- **R5:** **Easy and flexible deployment and operation:** From the service operator's point of view, mobile signature solutions should support an easy and flexible deployment as well as an efficient operation, in order to save installation, set-up, and operation costs.

Based on these requirements, we propose a generic and adaptable mobile eID and e-signature solution, which removes limitations of current solutions. We introduce and discuss the concept of our solution in the next sections before providing details on its implementation in Section VI.

IV. Architecture

As discussed in Section II, mobile eID and e-signature solutions follow either a SIM-based or a server-based approach to store eID data and to create electronic signatures. Other approaches would be possible on smartphones but cannot be applied on standard mobile phones due to their limited capabilities. Considering the requirements defined in Section III, we have decided to follow a server-based approach for our solution. This means, that a central hardware security module (HSM) stores all eID data and computes electronic signatures. Since solutions based on server-side signatures have very limited hardware requirements on the user side, they are comparatively cheap, user-friendly, and flexible in their deployment, as no roll-out of tokens is required (R2). There are no up-front investments in dedicated SIM cards and no requirements towards the MNOs, hence, the targeted user group is not limited to a single, or certain MNOs. Advantages of server-based signature-creation approaches in terms of usability and user acceptance have also been discussed by Zefferer et al. in [4]. Thus, reliance on a server-based approach assures that requirements regarding usability (R3) are met.

A theoretic concept of a server-based mobile signature solution and a solution to store users private keys in a secure manner on a remote server has been proposed by Orthacker et al. [12] in 2010. The proposed solution fulfills the requirements of *qualified electronic signatures* as defined by EU Directive 1999/93/EC [10], which emphasizes the suitability of this concept for security-critical application scenarios. Furthermore, a server-based mobile eID and e-signature solution that is compliant to the EU Directive 1999/93/EC has been in productive operation in Austria for several years. This provides evidence that server-based solutions are capable to meet given security requirements (R4).

On a high level view, our solution defines the three processes: *registration*, *activation* and *usage*. These processes have different properties regarding computational effort and security constraints. During registration, which is mainly a matter of legal and organizational requirements, the identity of the user is verified. Usually, it is sufficient to perform the registration only once per user. During activation, a new eID and a signing key and certificate are created for a registered user. Activation is required once per life span of an eID. In the usage process, created eIDs and signing keys are used by the user for authentication purposes and to create electronic signatures. Details of the three processes will be provided in the following section.

The architecture of our mobile eID and e-signature solution, which is shown in Fig. 1, basically reflects the three processes defined above. The entire architecture is split into an inner part and an outer part. Components implementing functionality of the activation and the usage processes are divided between these two parts. As shown in Fig. 1, each part has its own database to store required internal data.

This way, the architecture is mainly composed of two databases and the four core components *Activation Outer*, *Activation Inner*, *Usage Outer*, and *Usage Inner*. The split between inner and outer components is a security feature as it reduces the impact of a data loss in case a service connected to the outer world gets compromised. Communication between outer and inner components happens via a limited, pre-defined set of commands over an encrypted channel. The separation of the core components allows for a very flexible deployment where, e.g., the activation parts can run on different machines, a different network or, if the business process allows/demands it, without a remote access at all. Additionally, access rights can be granted more restrictively, as only the activation process requires write access to many fields in the databases. On the other hand, it is theoretically also possible to deploy the complete service on a single machine, if this is the preferred deployment scenario. This way, the chosen architecture meets the requirements of security (R4) and also the requirements for easy and flexible deployment, and efficient operation (R5).

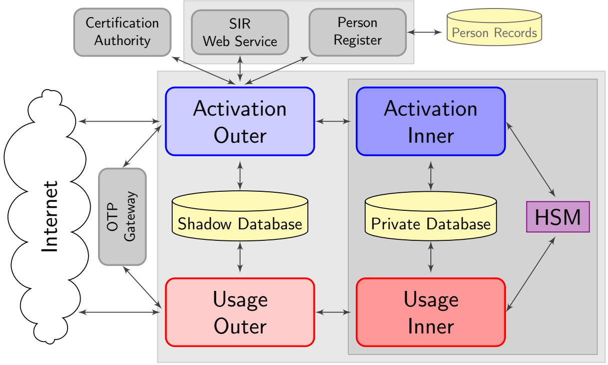


Figure 1: Overview of Core Components

In addition to the four core components, the proposed architecture additionally defines two internal and two external components. The external component *OTP Gateway* is required during the activation and the usage processes to send OTPs to users. The internal component *SIR Web Service* is used during the registration phase and is part of our solution. The *Person Register* and the *Certification Authority (CA)* are services that are required during the activation process. While the CA is an external component, the Person Register is an internal component, which usually connects to an external database. By clearly separating potential external components from the core components of our solution, we can meet the requirement for flexibility regarding external components already on architectural level (R1). The three processes, which build up our solution and cover its functionality as well as all involved components are described in the following section in detail.

V. Processes

The functionality of the proposed technology-agnostic mobile eID and e-signature solution is basically covered by the the processes, *registration*, *activation* and *usage*. The purpose of these processes is discussed in the following subsections in more detail.

A. Registration Process

During the registration process, the identity of a user is verified. Each user has to run the registration process once, before being able to use the proposed solution. In order to allow for a flexible setup of the registration process and to cover a broad range of legal and organizational requirements regarding the registration process, the registration process has been designed to support different types of registration. In particular, the following types of registration have been defined. These types of registration cover use cases from the e-government domain as well as use cases from related domains such as e-commerce or e-business. Also, the proposed architecture is flexible enough to allow for an easy integration of further alternative registration types, in case this is required by the given use case.

- **Registration via registration officer:** The registration officer (RO) is a trusted user, who verifies the identity of the user face-to-face using official IDs, e.g., a passport. After manual verification of the user's identity, the RO manually registers the user in the system.
- **Self registration:** Self registration is carried out by the user herself with the help of an existing eID (e.g., a smart card). The systems verifies the user's ID by means of the provided eID and afterwards registers the user.
- **Offline registration:** To support offline registration, the proposed solution supports registration of users via so-called *Standard Identification Records (SIR)*. A SIR contains information to identify a person, information about the ID used to verify the identity of the applicant, a binding towards a hardware token, i.e., a mobile phone for the use case at hand, and the digital signature of a RO or a trusted partner, e.g., a bank or a university. During the registration process, the system verifies the validity of a provided SIR that has been created offline, i.e. checks that the signature is valid and that the signer of the SIR is a legitimate RO or trusted partner.

Support of different types of registration allows for a very flexible setup of the registration process and covers a broad range of legal and organizational requirements regarding the registration process. This, in turn, contributes to a flexible operation of the proposed solution, which has been identified as key requirement (R5).

B. Activation Process

After successful registration, users can run the activation process to create a new eID. Our solution supports multiple eIDs for each user. Hence, the activation process can be run multiple times by each user. During the activation process, the unique identifier of the applicant is bound to the mobile phone, or more precisely, to the signing certificate that is issued during the activation process.

To activate a new eID, the applicant has to prove possession of the specified mobile phone. This is achieved by means of OTPs that are sent to the user through an OTP Gateway.

When the user has proven possession of her mobile phone, a signing key-pair is generated for the user inside the server-side HSM. The public key and the filtering criteria to find the applicant, e.g., name and date of birth, is sent to the Person Register. The Person Register is a component that connects to a database containing potential users of the service. Depending on the deployment and application scenario, this can be an existing official database like a central register of residence maintained by a public authority, an existing domain-specific database like the database of employees of a private-sector company, or a database specifically for this service that grows with every new registration.

If the user has been found unambiguously in the database, the Person Register returns a signed data structure that contains the unique eID of the applicant within the register and the public key of the created signature key-pair. Thus, it is possible to link a signature to a person for means of identification without the need to embed the unique eID directly in the signing certificate. By clearly separating eID functionality from e-signature functionality, users' privacy is assured. A similar concept is already successfully applied in existing national eID solutions [16].

Subsequently, a end-user certificate is requested from the certification authority (CA). The certificate, the wrapped private key, and the created eID data are stored encrypted in the database. The encryption of user data is based on a secret signature password, which the applicant chooses during the activation process. Our solution relies on hybrid encryption schemes, in order to encrypt data on behalf of the user without knowledge of the signature password. The decryption, however, requires the consent of the user, which she gives by providing the signature password. By choosing different signature passwords, a user can activate different eIDs for the same mobile phone number. Each eID can be managed separately. This enables users to have eIDs for different purposes, e.g., private and official purposes.

C. Usage Process

After successful completion of the activation process, the user can use the created eID and signing key to securely and conveniently authenticate at services and to create electronic signatures. To issue an electronic signature, the user has to enter her phone number and signature password. The signature password is used to decrypt a private key that is part of the hybrid encryption mentioned above. Thus, neither the activation of the user's signature key has to take place before the two-factor authentication is complete, nor must the signature password be stored in a session.

Next, the service sends a OTP via the OTP Gateway to verify possession of the mobile phone. After the user has been successfully authenticated, the user data is read from the database and decrypted using the user's private key of the hybrid encryption. Then, the still-wrapped private key of the signing key-pair is loaded into the HSM where it is unwrapped. Finally, the unwrapped key is used to create an electronic signature. After successful completion of the signature-creation process, the unwrapped key is discarded.

VI. Evaluation

Based on the proposed architecture, we implemented a prototype to evaluate and demonstrate the applicability of our solution. We built our implementation on a set of well-known and production-ready frameworks and libraries. The foundation of all modules is the Spring Framework [17], which greatly supports the development of modular and flexible software solutions. Access to databases happens through Hibernate [18], an object-relational mapping (ORM) library. Thus, the access to a database is mostly independent from its implementation. This gives us the freedom to adapt the databases to the needs of a certain deployment scenario. For cryptographic operations we use the IAIK JCE and iSaSiLk libraries [19]. Messages between the modules are exchanged using Apache ActiveMQ [20]. As means to deliver OTPs our implementation uses random transaction numbers (TAN) delivered by an SMS gateway.

To assure its security, we have assessed our implementation by means of a security analysis. To follow an approved approach, the implementation has been evaluated regarding the most recent critical risks according to OWASP [21] using a white-box testing approach. This approach allows the auditor having knowledge of the internal structure of the project, like the knowledge of libraries and frameworks in use, as well as having access to the source code.

The developed and assessed implementation covers the three processes defined in Section V. The realization of these processes is discussed in the following subsections.

A. Registration Process

In this step, the applicant has to prove her identity. Our implementation supports the three types of registration defined in Section V. In a traditional setup this happens at the office of the RO. For this scenario, our implementation provides a web-based UI, through which the RO can register the applicant in the system.

However, in some situations it might be beneficial if the RO travels from applicant to applicant (offline registration). We developed different front-ends to simplify this type of registration. Initially, we developed a simple, yet comprehensive, stand-alone application based on Spring MVC. This application can be used on mobile devices in case of traveling ROs and supports the RO in creating SIRs. Furthermore, we developed a proof-of-concept where a traveling RO takes the picture of the ID of an applicant. The required data is extracted using optical character recognition (OCR). Additionally, our implementation provides a web service that accepts these externally created SIRs.

To cover the third registration type, our implementation provides a UI for the applicant. This UI allows the applicant to carry out a self registration in case she has already a trusted eID (e.g., smart card).

B. Activation Process

In this step, the applicant creates and activates a new mobile eID. A pre-registered applicant can perform this step on her own and independent of the registration process.

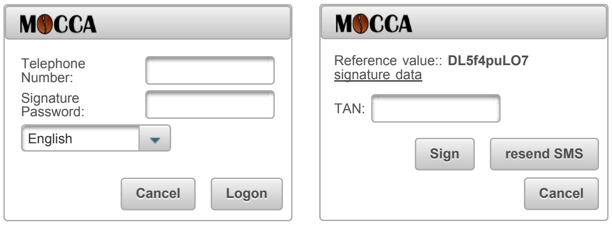
The activation process offers again a web-based interface. It has been developed using JSF 2.1 [22] and Primefaces [23]. The decision to use a different technology to create the UI is based on the rich set of UI components that is part of Primefaces. Thus, a flexible, easy to use, role/permission-based interface has been developed in a short amount of time.

Apart from the actual activation process, this module offers interfaces for several other tasks. Registration officers can perform activations on behalf of someone else. Hence, the activation process has been extended by the registration tasks. Furthermore, we developed interfaces to manage eIDs, both for the owner and a support team. An administration UI allows the definition and assignment of roles.

C. Usage Process

The usage process was developed alongside the activation and therefore is built on the same technologies, i.e., Java Server Faces [22] and Primefaces [23]. The interfaces are reduced to the bare minimum required for authenticating users and authorizing the creation of signatures. This facilitates an easy integration of our solution into arbitrary third-party applications. The two main forms for the two-factor authentication are shown in Fig. 2.

First, the signer provides her phone number and signature password. If the authentication was successful, two random



Reference value:: **DL5f4puLO7**

(a) Login

(b) TAN Verification

Figure 2: Interface of the Usage Process

values are generated: the reference value, which is shown in the TAN verification form (Fig. 2(b)) and in the SMS to provide a link between TAN and signature, and the TAN itself, which is only sent by SMS.

After verifying the reference value received by SMS against the reference value prompted in the TAN verification form, the user enters the received TAN. If the correct TAN is entered, the signature is created. This form also provides a link to display the signature data, to verify what data will be signed.

VII. Conclusions

In this paper, we have proposed an enhanced eID and e-signature solution. The practical applicability of the proposed solution has been successfully evaluated and demonstrated by means of a concrete implementation. A test deployment of this implementation is publicly available online and can be accessed for test purposes [24].

By relying on a server-side HSM for storage of users' eID data and for realization of cryptographic functionality, our solution is one of few mobile eID and e-signature solutions that rely on a server-based approach. In contrast to existing server-based eID and e-signature solutions, our solution has not been tailored to requirements of a specific use case or application scenario but has been based on an abstract architecture. This assures that the proposed solution is applicable for different use cases and fields of operation.

Furthermore, the proposed solution shows that secure two-factor based user authentication can be achieved in a user-friendly way and does not necessarily require the cumbersome handling of additional security tokens such as smart cards. This way, the proposed solution provides a promising way to enhance the usability of transactional e-government services while maintaining a high level of security.

Due to its easy integrability and high degree of usability, the proposed solution is not limited to e-government-related use cases. It can also be an attractive alternative for less security-critical services such as e-commerce or social networking. If also these services take the opportunity to provide users a higher degree of security while maintaining a high degree of usability by integrating the proposed mobile eID and e-signature solution, insecure password-based authentication schemes will hopefully be history in the future.

Acknowledgements: The authors have been supported by the European Commission Seventh Framework Programme through project *FutureID*, grant agreement number 318424.

References

[1] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, Apr. 2004, pp. 75–78. [Online]. Available: http://doi.acm.org/10.1145/975817.975820

[2] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proceedings of the 16th International Conference on World Wide Web, ser. WWW '07. New York, NY, USA: ACM, 2007, pp. 657–666. [Online]. Available: http://doi.acm.org/10.1145/1242572.1242661

[3] S. Arora, "National e-id card schemes: A european overview," Inf. Secur. Tech. Rep., vol. 13, no. 2, May 2008, pp. 46–53. [Online]. Available: http://dx.doi.org/10.1016/j.istr.2008.08.002

[4] T. Zefferer and V. Krnjic, "Usability evaluation of electronic signature based e-government solutions," in Proceedings of the IADIS International Conference WWW/INTERNET 2012, 2012, pp. 227 – 234.

[5] A. Ruiz-Martinez, D. Sanchez-Martinez, M. Martinez-Montesinos, and A. F. Gomez-Skarmeta, "A survey of electronic signature solutions in mobile devices." JTAER, vol. 2, no. 3, 2007, pp. 94–109. [Online]. Available: http://dblp.uni-trier.de/db/journals/jtaer/jtaer2.html#Ruiz-MartinezSMG07

[6] "Handy Signatur und Buergerkarte," 2013, [retrieved: November, 2013]. [Online]. Available: http://www.buergerkarte.at/

[7] "Estonia eID," 2013, [accessed November, 2013]. [Online]. Available: http://www.id.ee/?lang=en

[8] "Belgium eID," 2013, [accessed November, 2013]. [Online]. Available: http://eid.belgium.be/en/

[9] "Spanish eID," 2013, [accessed November, 2013]. [Online]. Available: http://www.dnielectronico.es/

[10] European Parliament and Council, "Directive 1999/93/ec on a community framework for electronic signatures," December 1999.

[11] E. Pisko, "Mobile electronic signatures: Progression from mobile service to mobile application unit." in ICMB. IEEE Computer Society, 2007, p. 6. [Online]. Available: http://dblp.uni-trier.de/db/conf/icmb/icmb2007.html#Pisko07

[12] C. Orthacker, M. Centner, and C. Kittl, "Qualified mobile server signature," in Security and Privacy – Silver Linings in the Cloud, ser. IFIP Advances in Information and Communication Technology, K. Rannenberg, V. Varadharajan, and C. Weber, Eds., vol. 330. Springer Berlin Heidelberg, 2010, p. 103–111. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-15257-3_10

[13] "Estonia mobile eID," 2013, [accessed November, 2013]. [Online]. Available: http://mobiil.id.ee/

[14] "Norway eID," 2013, [accessed November, 2013]. [Online]. Available: https://www.bankid.no/

[15] "Austrian Handy Signatur," 2013, [accessed November, 2013]. [Online]. Available: https://www.handy-signatur.at/

[16] H. Leitold, A. Hollosi, and R. Posch, "Security architecture of the austrian citizen card concept," in Proceedings of 18th Annual Computer Security Applications Conference (ACSAC'2002), Las Vegas, 9-13 December 2002. pp. 391-400, IEEE Computer Society, ISBN 0-7695-1828-1, ISSN 1063-9527., 2002.

[17] "Spring Framework," 2014, [accessed November, 2013]. [Online]. Available: http://projects.spring.io/spring-framework/

[18] "Hibernate," 2014, [accessed November, 2013]. [Online]. Available: http://hibernate.org/

[19] "IAIK JCE," 2014, [accessed November, 2013]. [Online]. Available: http://jce.iaik.tugraz.at/

[20] "Apache Active MQ," 2014, [accessed November, 2013]. [Online]. Available: http://activemq.apache.org/

[21] The Open Web Application Security Project, "Owasp top 10 - 2013 the ten most critical web application security risks," 2013.

[22] "Java Server Faces," 2014, [accessed November, 2013]. [Online]. Available: https://javaserverfaces.java.net/

[23] "Primefaces," 2014, [accessed November, 2013]. [Online]. Available: http://www.primefaces.org/

[24] "Test deployment of our implementation," 2014, [retrieved: November, 2013]. [Online]. Available: https://pheasant.iaik.tugraz.at:8443/Registration/

An Infrastructure for Community Signatures and Micro-Agreements

Architecture, Android prototype implementation, and usage examples

Mitja Vardjan and Jan Porekar
Research Department
SETCCE
Ljubljana, Slovenia
{mitja.vardjan, jan.porekar}@setcce.si

***Abstract*—Digital signatures are widely used for non-repudiation and other purposes. In various cases, there is a group of two or more parties that have to agree on a common set of data and digitally sign it in order to provide the other party or parties a proof of non-repudiation. A simple and scalable infrastructure for community signatures or groups of individual party signatures is described. It allows third party applications to simultaneously digitally sign arbitrary XML documents by any number of entities, for any purpose, using high level interfaces, not having to deal with digital signatures themselves. A dedicated backend server dynamically merges received documents and signatures from all parties. When a sufficient number of entities have signed the document, a signal is triggered to announce the document finalization. Despite the simple overall design, handling security issues and user control at appropriate spots are crucial for any business application.**

Keywords-community; agreement; digital signature; mobile environment

I. Introduction

One of the most used aspects of digital signatures is non-repudiation. When electronic documents are digitally signed by one or more parties, the signatures can be used to verify the document integrity and, more importantly for this work, to prove that the parties have agreed on the document and stand behind it.

In many cases, only one valid digital signature is provided with the document at any time. The goal in such cases is usually to ensure document integrity, or to provide non-repudiation of a single entity. In case of signing contracts, agreements, and similar documents, two or more entities are to provide non-repudiation to each other. Some of these entities can be owners of internet connected pervasive services or internet connected objects. The signing process and distribution of digital signatures can easily get overly complex or even infeasible for the entities, especially if their number is large or arbitrary. This can be remedied in a business process where the document format and the order, in which it is signed by the entities, are determined by the application or protocol, such as the negotiation presented in [1].

The infrastructural service described here allows for groups and communities to reach legally binding agreements in an ad-hoc manner. Third party services can offload any documents that need to be agreed over group of participants or even whole communities. These documents range from service level agreements, meeting minutes to non-disclosure agreements or even business contracts that may have rich content embedded. The work in this paper is a continuation and complement of [1].

The functionality reuses the concepts of digital identities, certificates and digital signatures. Documents are structured with Extensible Markup Language (XML) and agreements are signed using XMLDSig [5]. Both architecture and implementation target mobile and pervasive environments by providing an asynchronous and scalable solution that limits bandwidth usage, avoids unnecessary communication, and enables all user devices to be used from arbitrary local networks that are connected to the Internet intermittently and through firewalls.

Existing group signature and concurrent signature [13] solutions, especially the improved and multi-party versions [14][15][16] fit various purposes, but may not be most suitable for use by third party application developers who prefer well known solutions and expect fast and easy integration. Some existing designs for group signature use their own custom signatures and require additional solution-specific steps to sign the data and to verify a signature [7][8][9], or allow only community members to sign [8], which is not suitable for ad-hoc communities. Such requirements can put additional burden to both implementation of third party applications that use the signature infrastructure, and to community administration. In terms of efficiency and optimization, additional network interactions are required, e.g., when the keystone is released in case of concurrent signatures. Moreover, both group signatures and concurrent signatures diverge even further from the traditional way of signing paper documents, still widely used. While the concept of fair exchange of signatures and decreased verification time are highly beneficial in some cases, the additional differences may present an obstacle for adoption of the solution. For example, if the identity of the first signers is not known to all, subsequent signers may be less likely to sign the document. This may be because in case of known identities, they trust the party or parties who already signed the document, or simply because they have a proof that the party with known identity has already signed the document, e.g., when negotiating a service-level agreement [1]. On the other hand,

ISBN: 978-1-61208-324-7

for communities where all members are equal and do not know or trust each other, the concurrent signatures are better in terms of fairness and non-exposure, but they are not used in the presented work.

The next chapter describes the initial document creation and its distribution to other users. The chapter is followed by descriptions of document signing and finalization procedure. Afterwards, various privacy and security aspects of the whole process are explained. The paper ends with usage examples to illustrate a few implemented and suggested services that are using the presented community signature infrastructure.

II. Document Creation and Distribution

Initially, an XML document with arbitrary schema and contents is created either by one party or in a collaborative manner by multiple members of a community. The document may hold a service level agreement, meeting minutes, non-disclosure agreement, or even business contracts that may have rich content embedded such as images, video or voice recording.

Regardless of what the document represents, the community members are expected to review it once it is finalized and confirm they agree with it. Their consent is formally expressed with their digital signature, appended to the document as a detached XMLDSig [5]. Depending on the application, a member may choose to sign the whole document, only some of its parts, or nothing and leave the document intact.

The initial document is distributed to the intended signers or members by uploading it to a dedicated Representational State Transfer (REST) server in a single HTTP PUT request. The REST server stores the document under the name, supplied by the client as resource name within the URL. The name is generated as a random string of a fixed length. The concept of resource name is similar to universally unique identifier (UUID) [2] but the name is shorter because it is checked for uniqueness at the server level when the resource is initially uploaded. Unless a resource with same name already exists on the server and the HTTP PUT request has to be repeated with a new name, the upload is a single step operation. The request includes the owner's serialized X.509 certificate [4] as part of the URL. This certificate is stored by the server for later authorization to access the document by others. It is never used to sign the document, unless the user chooses to do so. Therefore, it could be anonymous or generated ad-hoc by the initial document uploader. Its corresponding private key is used to sign the resource name. This signature is not supplied with the initial upload, but with another URL, generated by the community signature infrastructure.

Whenever a document is downloaded or a new version of existing document is uploaded, digital signature of resource name is passed as a URL parameter. The same URL is used for downloading and updating documents. The URL of the uploaded document is distributed to the members as an invitation for them to agree with and digitally sign the document.

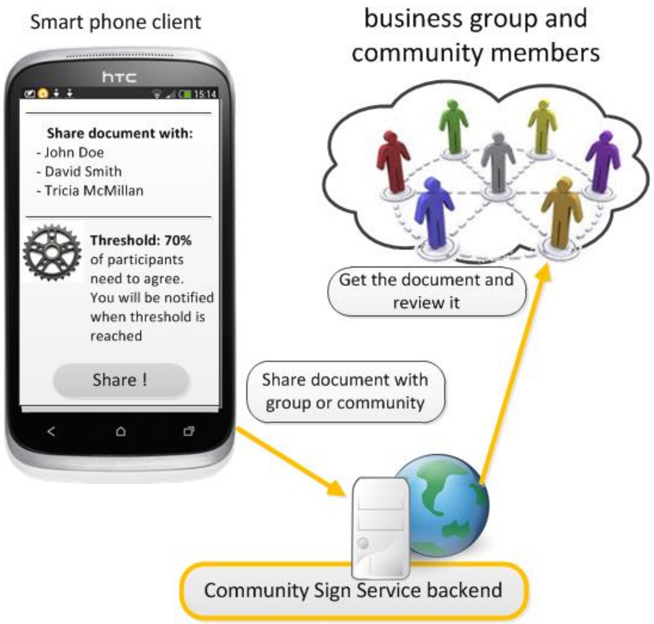

Smart phone client
business group and community members
htc
15:14
Share document with:
- John Doe
- David Smith
- Tricia McMillan
Threshold: 70%
of participants need to agree.
You will be notified when threshold is reached
Share !
Get the document and review it
Share document with group or community
Community Sign Service backend

Figure 1. Document creation and distribution.

The members list is usually application specific and the URL distribution is handled in the background by an app that is using the community signature infrastructure. If this is not the case, the URL and the document can still be accessed manually within the signature infrastructure itself (Figure 4). This lightweight and easy to implement process is suitable for the uploader device and signer devices, which are usually smart phones or tablet PCs. When a user chooses to reject or ignore the invitation to sign the document before he even reads it, bandwidth usage is negligible.

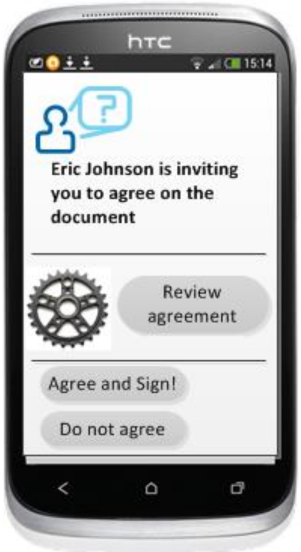
III. Micro-Agreements and Document Finalization

In the process of agreeing, the canonical form [6] of agreement document is digitally signed with a private key that is stored in participant's smart phone's secure storage. The meeting participants do not need to sign the document immediately but can postpone the signing of the agreement.

After the agreement is signed by a participant it is uploaded back to the community sign service using the same URL that has been used to download it. The reasoning is that for community signatures, anyone who is authorized to download the document should be able to upload the signed version as well. If this is not the case, the concept of authorization signature in the URL can be easily expanded to include option to allow download only or both upload and download. An example solution is to sign document resource name, suffixed with an appropriate parameter, known to the service. The community sign service at the REST server verifies whether the digital signature is valid and whether the content of the agreement has not been modified in any way.

The community signature functionality allows third party services that are using it to specify the minimal number of community members that need to agree in either relative terms such as percentage of community or fixed threshold numbers. Every time the document with a new signature is uploaded to the community signature service backend node, this micro-agreement is merged into the main document stored on the server. Due to the nature of detached XMLDSig, the merges originating from various signers can be performed in any given order and the signers will experience a convenient and seemingly parallel signing procedure.

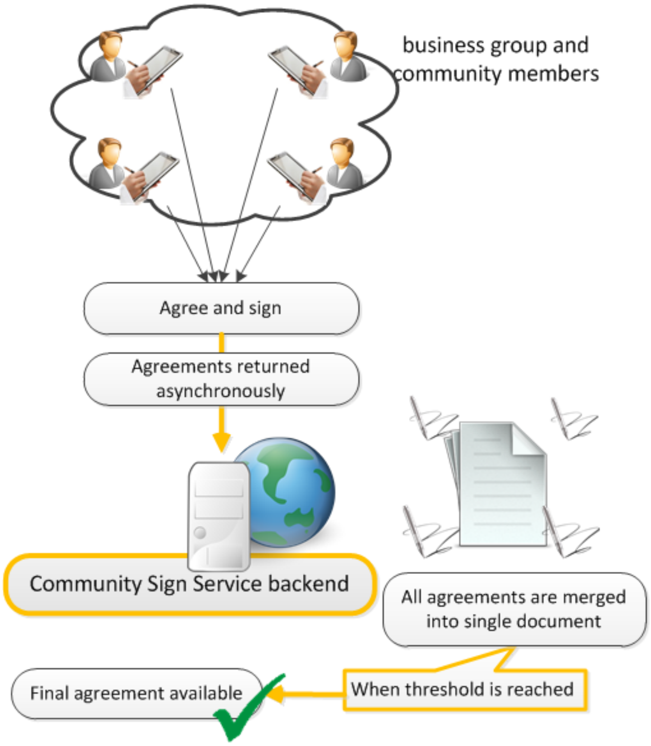
The resulting document at any moment contains signatures from all parties that have signed the document and sent it back to the server so far. When number of parties that signed the document exceeds the given threshold, the community signature service backend server signals completion and participants can now download the final agreement, which now contains at least the required number of signatures (Figure 3) and represents a common and a legally valid agreement. Depending on the implementation, the document finalization can be signaled to the original document creator, e.g., meeting organizer, who can first inspect the document and the signers and then choose to signal document finalization to the other selected parties. At any point, the parties can see the current status of any document they have signed, or were invited to sign. Figure 4 shows the status of a document in the process of being signed (left) and the status of that same document at a later time, when one more party has signed it and the number of signers reached the required threshold (right). If concurrent signatures were used, full status with signers' identities could be displayed only after the keystone is released.



Eric Johnson is inviting you to agree on the document

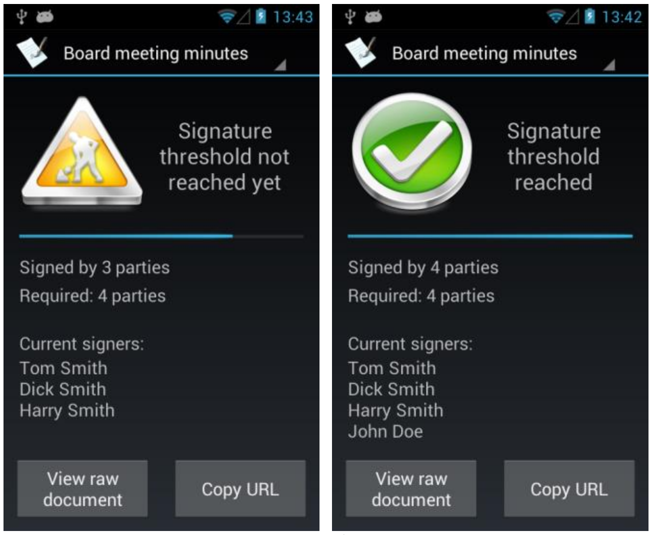
Figure 2. A community member receives invitation to sign a document.

Unlike a group signature [7] where multiple individual signatures are replaced with a single group signature, individual signatures are preserved and any party can verify individual signatures using a standard verification procedure. Due to the nature of XMLDSig, any party can also get the list of all signers solely from the document.



business group and community members
Agree and sign
Agreements returned asynchronously
Community Sign Service backend
All agreements are merged into single document
When threshold is reached
Final agreement available

Figure 3. Community signature and document finalization.



13:43

Board meeting minutes

Signature threshold not reached yet

Signed by 3 parties
Required: 4 parties

Current signers:
Tom Smith
Dick Smith
Harry Smith

13:42

Board meeting minutes

Signature threshold reached

Signed by 4 parties
Required: 4 parties

Current signers:
Tom Smith
Dick Smith
Harry Smith
John Doe

Figure 4. Viewing current status of the document signing process.

The downside of not using the concept of group signature [7] is that processing power and time to verify all signatures increase with number of signatures in the final document. As the increase is only linear, this is usually not problematic in terms of scalability. If all parties can be forced to use a specific key-pair type, then verification of multiple signatures could be sped up [10][11], although care must be taken because some such solutions have issues [12].

IV. Privacy and Security Aspects

The two main groups of information that could be treated as sensitive are the document contents and the list of entities who have signed the document. The document itself has to be made fully available to all entities that are given the option to sign it. Same applies to the list of signers because they all receive the final document in the end, leaving no alternative to ultimately trusting the entities not to disclose any sensitive information they receive.

Various notifications about document finalization do not carry any personal or document data and usually do not need to be secured. A few other points where it makes sense to take security into account are described below.

A. *Document Distribution*

There are established protocols to encrypt the network traffic from eavesdropping. However, a custom solution described in Chapter II is used as a secure and convenient method to authorize the clients to download and upload the document. With the proposed solution, the clients (entities) are given only one URL that already contains all necessary tokens (Figure 5). As the digital signature of requested resource is part of the URL, the certificate owner can easily disable access by removing the public part of his certificate at the service backend (Figure 1 and Figure 5).

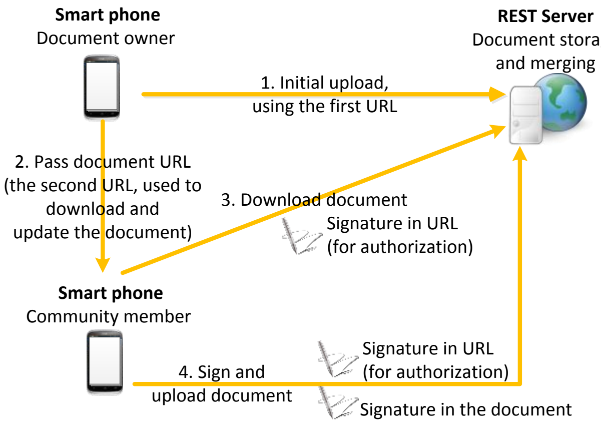


Figure 5. The two roles of signatures.

Alternatively, when the certificate is revoked, access is automatically disabled, provided that the service backend implementation does check certificate revocation lists.

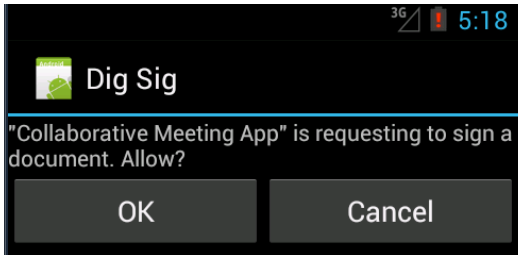
In any case, the number of network operations from mobile devices is limited and the authorization is integrated into the simple and widely used HTTP methods, so third party developers are not required to implement any authorization procedures.

B. *Storage of Certificates on Android*

With any digital signature based system, it is vital to protect the private keys from unauthorized use. The prototype has been implemented for Android where a secure storage is provided by the operating system. This storage is used for storing user's certificates and private keys. It is accessed in two significantly different ways, depending on Android version. For Android versions up to 4.2.2, the API is not public and the operating system grants requests to the storage based on the requestor process ID. The concept is described in [1]. For Android versions 4.3 and newer, the access to the secure storage is possible only through the new and official API for storing and accessing certificates and keys. To support all versions, the app implements both strategies and chooses the appropriate one dynamically.

C. *Using the Securely Stored Private Keys on Android*

To sign an arbitrary XML document, our prototype app can be used directly. However, in most cases it is to be used by other apps that parse the document and show the user a human readable and application specific document representation before the user authorizes signing. The problem is to access the user's private keys, which are not available to third party apps and not even to the operating system. As a solution, the third party app can simply invoke in the background our prototype app with access to private keys to sign the given document.



"Collaborative Meeting App" is requesting to sign a document. Allow?

Figure 6. Third party app requests to sign a document have to be explicitly confirmed by the user.

It is vital for the prototype app to show the user which app is trying to sign the document in the background, to prompt the user to authorize signing (Figure 6) and choose the identity to use (if multiple certificates are stored). The key itself is never exposed to third party apps, so only the data explicitly approved by the user are signed.

V. USAGE EXAMPLES

Examples of usage are described below. The community micro-agreements are suited to also be used by applications and services that enable governance tools to communities.

A. *Capturing Meeting Minutes*

Community micro-agreements allow business communities to capture meeting minutes and other meeting agreements in a legally valid and binding manner. The meeting organizer can choose whether the consensus is reached among only participants that are physically present during the meeting or the whole community.

Existing community signature prototype implementation has been used by an example app to capture meeting minutes. After users register to the meeting through this app, they can actively participate in the meeting. Their input is recorded by their Android devices and sent to a central Android device, which has the role of the document owner. When the meeting is finalized on that central device, the minutes are uploaded to the document storage server (Figure 7) and its URL is distributed to meeting participants. The REST servers which handle distribution of document URLs and receive notifications about document finalization (Figure

7) are application specific, i.e., implemented as part of the meeting minutes software, not the general community signature software. Google Cloud Messaging (GCM) is used to relay the messages to Android phones of users who are to sign the minutes. At an earlier point, the meeting software automatically registers Android devices of community members with GCM to receive these messages. GCM is used by the meeting software as a convenient way to push small messages to Android devices, connected to the Internet through firewalls, with variable network addresses, etc. The community signature infrastructure does not require using neither GCM, nor the additional REST server to distribute document URL, but only to distribute the URL to community members. Therefore, any alternative distribution of the URL is valid. For example, the app on the central device embeds the URL into a Quick Response Code (QR code) and the physically present members can scan it. Again, this is only an alternative way of URL distribution and the primary way is application specific automatic distribution in the background, in this case through GCM. Arrows in Figure 7 indicate information flow for the implementation with GCM, starting with document upload by the document owner to the first REST server shown at the top center.

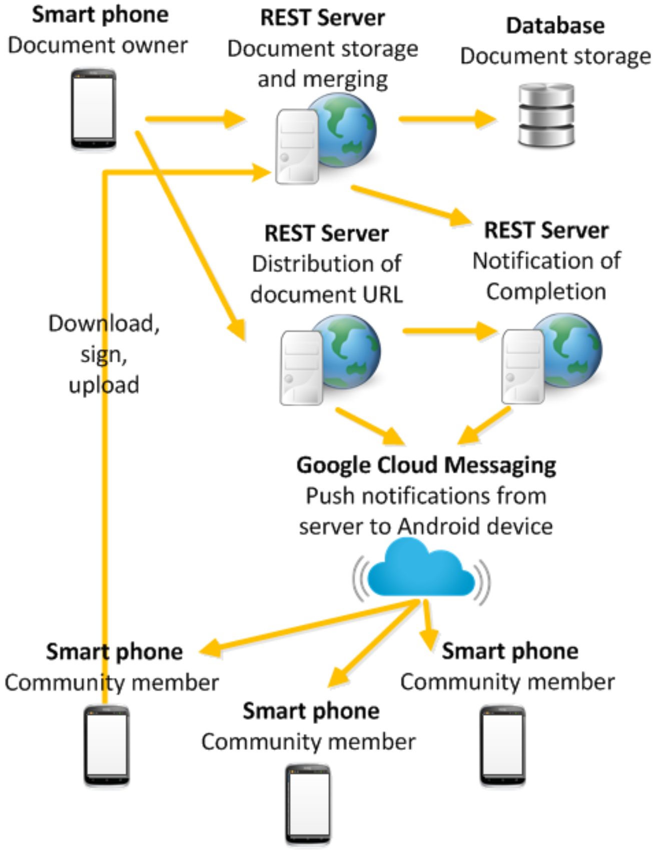
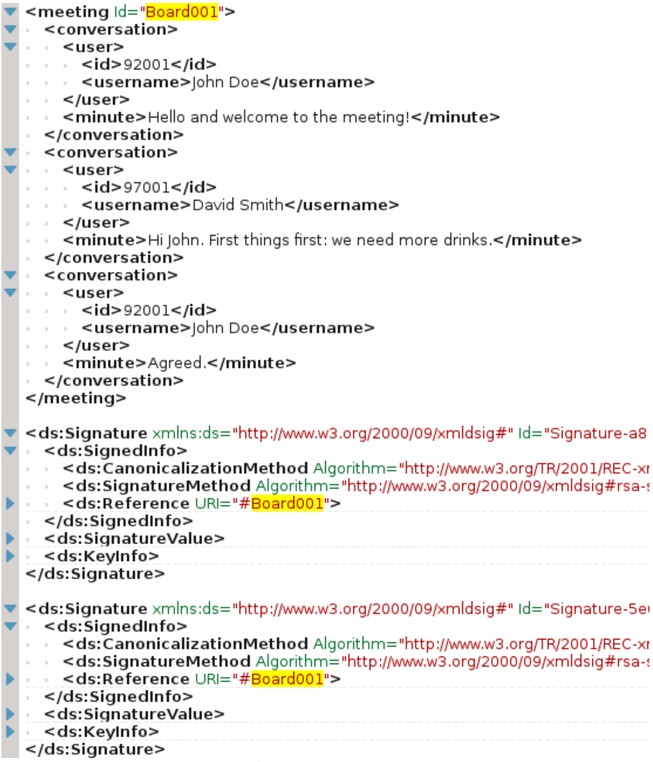


Figure 7. Process and information flow between devices in a chosen implementation for capturing meeting minutes.

Regardless of the implementation, the signatures are always in standard XMLDSig form, as in Figure 8. In the figure, XML nodes with signature and certificate values are collapsed but the highlighted text shows the signatures refer to the whole document, i.e., the whole meeting minutes. In case a participant agreed only with part of the document, his signature would refer to the relevant part only, provided that the application specific implementation allowed signing only a part of the document.



```
<meeting Id="Board001">
  <conversation>
    <user>
      <id>92001</id>
      <username>John Doe</username>
    </user>
    <minute>Hello and welcome to the meeting!</minute>
  </conversation>
  <conversation>
    <user>
      <id>97001</id>
      <username>David Smith</username>
    </user>
    <minute>Hi John. First things first: we need more drinks.</minute>
  </conversation>
  <conversation>
    <user>
      <id>92001</id>
      <username>John Doe</username>
    </user>
    <minute>Agreed.</minute>
  </conversation>
</meeting>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-a8
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-x
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
    <ds:Reference URI="#Board001">
  </ds:SignedInfo>
  <ds:SignatureValue>
  <ds:KeyInfo>
</ds:Signature>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-5e
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-x
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
    <ds:Reference URI="#Board001">
  </ds:SignedInfo>
  <ds:SignatureValue>
  <ds:KeyInfo>
</ds:Signature>
```

Figure 8. An example of meeting minutes signed by two parties.

In this example, the omnipresent issue of identity mapping is evident. Mapping between various identity types is essential for any legally binging document. Typical identity types relevant for community signatures are:

- Possible identities in the signed document. Figure 8 shows a case where identities are explicitly listed in the signed document. This is not always the case. The document could include only impersonal statements.
- Identities in encoded X.509 certificates, contained in the collapsed “ds:KeyInfo” nodes in Figure 8.
- Identities of the community members who signed the document.

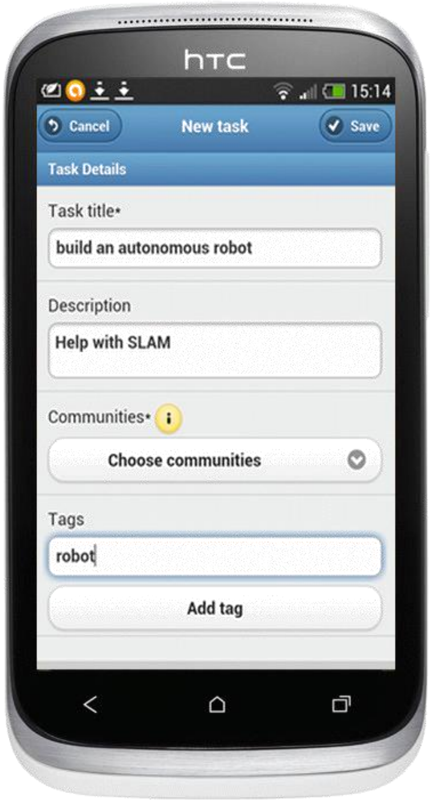
Clearly, any implementation should check:

- mapping between the certificate filed values, e.g., common name, and the document identities, if any,
- certificate validity and whether it is issued by a trusted authority,
- mapping between certificate and real entity, e.g., by checking the entity listed in the certificate is actually a member of the community that is supposed to sign the document.

For large communities, this can be far from trivial, as the certificate identities can be ambiguous and also because a single entity can be listed under different names in the certificate and community members list.

B. Crowd Tasking

A service called Crowd Tasking has been developed to enable community members to create tasks (an example is shown in Figure 9), propose solutions, post comments and solve tasks. These tasks usually involve some physical presence of people or physical work, which makes it inconvenient or impossible to post either the solution, or proof of the task solution to the service or to the Internet.



Task title•
build an autonomous robot

Description
Help with SLAM

Tags
robot

Figure 9. Crowd Tasking Service.

The service will integrate with the community signature infrastructure to enable task members to sign the agreements about the work to be done by each of them and to enable task creators to confirm the task completion by additional signature. As with any other usage of community signature, the interactions of third party service with community signature infrastructure and the document signing happen in the background, except prompting the user to confirm signing.

C. Service Sharing Within a Community

The policy negotiation described in [1] could be extended by integrating with community signatures and micro agreements presented here. A service provider would negotiate a service level agreement (SLA) with a community instead of only a single service consumer. The community members would decide if a particular SLA is compatible with community's internal rules and sign the SLA so the service could be shared within the community.

VI. CONCLUSION AND FURTHER WORK

An infrastructure and prototype implementation of community signatures and micro-agreements has been presented, followed by usage examples. The design uses digital signatures to sign XML documents, which can serve as legally binding agreements. It is based on REST servers, a database or other storage system, and Android devices. The simple, scalable and generic main concepts allow for fast integration of various third party services with it. Network communication is optimized for mobile devices with limited and intermittent bandwidth, but at least occasionally working network connection is still required for all devices. Compared to concurrent signatures, the presented approach requires slightly less network interactions, is more similar to traditional signing process of paper documents, and as such does not exchange signatures between parties in a fair manner, which has both advantages and disadvantages. Ideally, the solution could offer both signature options to cover additional possible scenarios. Other services are planned to use the implemented community signature infrastructure in an application specific manner.

ACKNOWLEDGMENT

Authors would like to thank the SOCIETIES project [3] consortium and EC for sponsoring the project.

REFERENCES

[1] M. Vardjan, M. Pavleski, and J. Porekar, "Securing Policy Negotiation for Socio-Pervasive Business Microinteractions", SECURWARE 2012: The Sixth International Conference on Emerging Security Information, Systems and Technologies, ISBN: 978-1-61208-209-7, Aug. 2012, pp. 142-147.

[2] ITU Recommendation X.667 (09/04), http://www.itu.int/rec/T-REC-X.667-200409-S/en [retrieved November, 2013].

[3] Self Orchestrating CommunIty ambiEnT IntelligEnce Spaces (SOCIETIES), EU FP7 project, Information and Communication Technologies, Grant Agreement Number 257493.

[4] X.509 standard recommendation, http://www.itu.int/rec/T-REC-X.509/en [retrieved November, 2013].

[5] XML-DSig, XML Signature Syntax and Processing, 2nd Edition http://www.w3.org/TR/xmldsig-core/, [retrieved April, 2012].

[6] Canonical XML 1.1, W3C recommendation, http://www.w3.org/TR/xml-c14n11/, [retrieved April, 2012].

[7] L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multisignature", IEE Proceedings - Computers and Digital Techniques, Volume 141, Issue 5, Sep. 1994, p. 307-313, DOI: 10.1049/ip-cdt:19941293.

[8] C. M. Hsu, S. H. Twu, and H. M. Chao, "A Group Digital Signature Technique for Authentication", IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, ISBN: 0-7803-7882-2, Oct. 2003, pp. 253 – 256.

[9] L. Harn, C. H. Lin, and C. W. Hu, "Contract Signatures in E-Commerce Applications", International Conference on Broadband, Wireless Computing, Communication and Applications, Nov. 2010, pp. 384-388, DOI: 10.1109/BWCCA.2010.101.

[10] C. Li, M. Hwang, and S. Chen, “A batch verifying and detecting the illegal signatures”, International Journal of Innovative Computing, Information and Control, Dec. 2010, pp. 5311-5320.

[11] A. Atanasiu, “A New Batch Verifying Scheme for Identifying Illegal Signatures”, Journal of Computer Science and Technology, Vol. 28, Issue 1, Jan. 2013, pp. 144-151.

[12] M. S. Hwang and C. C. Lee, “Research Issues and Challenges for Multiple Digital Signatures”, International Journal of Network Security, Vol.1, No.1, Jul. 2005, pp.1-7.

[13] L. Chen, C. Kudla, and K. G. Paterson, “Concurrent Signatures”, Advances in cryptology - EUROCRYPT 2004, Vol. 3027, May 2004, pp. 287-305.

[14] X. Tan, Q. Huang, and D. S. Wong, “Concurrent Signature without Random Oracles”, IACR Cryptology ePrint Archive, 2012.

[15] C. Shieh, H. Lin, and S. Yen, “Fair multi-party concurrent signatures”, Proc. of 18th Cryptology and Information Security Conference, 2008, pp. 108-118.

[16] J. Xushuai, Z. Zhou, W. Qin, Q. Jiang, and N. Zhou, “Multi-Party Concurrent Signature Scheme Based on Designated Verifiers”, Journal of Computers, Vol. 8, No. 11, Nov. 2013, pp. 2823-2830.

Human-Centered Ontology Engineering in E-Government Environments

Richard Siegl, Bernd Stadlhofer, and Peter Salhofer
FH JOANNEUM
University of Applied Sciences, Graz
emails: {richard.siegl.aim11@fh-joanneum.at, bernd.stadlhofer@fh-joanneum.at, peter.salhofer@fh-joanneum.at}

***Abstract*—Ontology engineering is a relatively new field in computer and information sciences. Its primary goal is to develop methodologies for modelling and building ontologies. These ontologies represent knowledge as a set of concepts within a specific domain. A common problem is, though, that it is almost impossible for domain experts to design and model their own ontology in the domain of E-Government without having the basic knowledge of computer science, especially in the field of ontology engineering. The goal of this paper is to describe, how the Rich Ontology Creation Kit for E-Government Transition (ROCKET), an ontology creation tool based on the Eclipse RCP framework, supports legal experts to bridge the gap between domain and technical specialists. To accomplish that goal, the web application SeGoF is described, which uses ontologies as an input for the automatic generation of E-Government forms based on semantic descriptions. Moreover, the methodology "Ontology Driven E-Government" is explained, as well as, the applied human-centered approach in ROCKET. As a result, the tool ROCKET allows domain experts to design and model ontologies in a convenient way by hiding the ontology language. It basically offers an easy-to-use graphical user interface, including wizards and editors like the axiom modeler to create the necessary elements to model an ontology.**

Keywords-SeGoF; ROCKET; ontology; engineering; ontology modelling; semantic MDA; e-government; domain modelling.

I. Introduction

Basically, ontology engineering is a relatively new field in computer and information science. Its goals are to develop methods and methodologies for building ontologies which formally represent knowledge as a set of concepts within a specific domain and its relationship to other concepts. These ontologies can be very useful in different situations, for example, when designing semantic web applications, like SeGoF [2].

However, the problem is that it is nearly impossible for users to formally express an ontology for a specific domain without having basic knowledge of computer science, especially in the field of ontology engineering. Therefore, tools and methods are required to help users to engineer their own ontology. Basically, there are at least two different roles which are involved in the process of creating ontologies: one domain expert and one technical expert. The domain expert has the required knowledge of a specific field and the technical expert understands the required concepts of ontology engineering. Both roles are interdependent and essential to create and model ontologies.

This paper focuses on the field of E-Government, more precisely, on the SeGoF web application and its requirements concerning ontology engineering. Therefore, SeGoF is described, as well as the different approaches like semantic MDA and ODEG. As a next step, the human-centered ontology engineering approach will be explained, covering the motivation behind this approach and other available methodologies. The next section covers the ODEG modelling process including all relevant process steps. In the following and last section of this paper, some of the most important features of ROCKET will be presented and explained, how they work.

II. Semantic eGovernment Forms (SeGoF)

Classical E-Government solutions are mostly aligned along conventional administrative processes. Hereby, a paper-driven workflow of these processes is the normal way to reflect these tasks. The paper-based application form is than simply replaced by an electronic web-form. As a consequence, the process behind these electronic web-forms is very important because it influences the usability and acceptance of the solution, but the prospects of those classical E-Government web-forms are often very limited. Furthermore, different administrative procedures are usually characterized by a set of rules and constraints which have to be met to make a user eligible for a specific service. In classic E-Government environments, the knowledge about these rules is mostly expressed programmatically but not semantically, which is a limiting factor.

A. Semantic MDA for e-government

As mentioned by Salhofer and Stadlhofer [1], this specific approach applies the basic principles of MDA (Model Driven Architecture) [1] in combination with a semantic model to the creation of E-Government services. The goal of this intention is that these services will then be available as semantic web services which can be searched for meeting the current goal or desire of a citizen. To be successful, it is important that all required artifacts are automatically generated from the model and that there is no need for manual coding. This enables very short development cycles and very fast adoption to shifting requirements, which is important because public agencies are facing significant budget cuts. As a consequence, resources have to be used as effective and efficient as possible [1].

B. ODEG

The goal of Ontology Driven E-Government (ODEG) [2] is to model ontologies for the E-Government domain which act as a basis for an integrated E-Government environment. The most important point is that these ontologies can be used to assist a citizen by formally expressing a goal that can be used for service discovery and it can also be used to express the necessary input of services which will be used for the subsequent form generation. The collected input data is transformed into a common data interchange standard format, and then, forwarded to the service oriented architecture (SOA) backend which executes the business process [2]. Furthermore, ODEG can be seen as an ontology engineering methodology because its main goal is to model ontologies for the E-Government domain by proving a human-centered approach.

As mentioned by Stadlhofer et al. [2], every relevant public service is semantically modeled and contains references to the required input elements. Moreover, every constraint on the service input element can be expressed by different semantic rules and can be evaluated by semantic reasoners. This allows an automatic creation of forms, for example web forms, and also plausibility checks of data gathered directly from the user. With this approach, the entire logic is now consistently kept in the semantic model. Additionally, another advantage of this approach is that the knowledge of public services becomes available in a machine processable form which allows more functionality than only form creation [2].

III. Human-centered ontology engineering approach

Nowadays, it is wildly argued that ontologies are the primary key to success concerning the realization of the semantic web. As a result, the ontology engineering process plays an important factor when designing and modelling ontologies. Thus, different methodologies were created to support and to document this process. This subchapter examines different approaches and explains the most important facets of the respective methodology. Basically, the focus lies on the investigation of the Ontology Driven E-Government (ODEG) methodology because ROCKET supports the ODEG modelling process and a human-centered approach by empowering legal experts. First of all, it is important to describe the motivation and requirements behind these methodologies.

A. Motivation

This section describes the motivation and the requirements concerning the E-Government domain derived from the SeGoF platform. These requirements refer to the ontology engineering methodology which is mandatory to achieve a well-defined and structured ontology building process and to support domain experts (or legal experts in case of the E-Government domain), so that they can design, model, and build ontologies autonomously without help from technical experts.

1) Domain expert centered approach: The methodology basically has to offer a domain expert centered approach which is the basic top-level goal. The intention of this approach is to empower legal experts so that they can design, model and build ontologies themselves. To realize this intention, the methodology has to support this approach concerning the respective process and by offering tool support which guides users through the building process.

2) Developed for electronic service provisioning in public administration: First of all, the application area of the ontology engineering methodology is important. In case of the SeGoF platform, the domain of E-Government is the respective target area. In general, it should be designed for electronic service provisioning in the context of public administration.

3) Clear and consistent process: The desired ontology engineering methodology should offer a clear and consistent process which guides users through the ontology building procedure. Usually, the process refers to the ontology building life cycle and consists of different phases. Besides the ontology modelling process, it may be important to cover the resulting project management of the project. This for example includes specification phases which covers the possibilities of knowledge retrieval.

4) Tool support: To realize the domain expert centered approach, the desired methodology should offer tools which support users during the ontology creation process. Basically, the tool has to hide the used ontology language behind a graphical user interface. With the help of certain templates, users are guided through the ontology building process. In the best case, legal experts should be able to implement and test the modelled ontology immediately.

5) Consideration of a possible collaborative construction: An essential aspect in the context of public administration is the consideration of legal certainty. In that case, legislation and enforcement of law on all governmental levels has to be ensured. As a consequence, this requires collaboration with a variety of different legal experts. That implies that the ontology creation tool should support and process a collaborative approach, which allows legal experts to collaboratively model, implement, verify and maintain ontologies.

B. Methodologies in the context of public administration

Concerning this paper, the target field in which respective methodologies have to be applied is public administration, more precisely E-Government and electronic public service provisioning. So the question is, which of the listed methodologies is capable of meeting the requirements. To answer this question, Stadlhofer et al. [3] conducted an analysis on different ontology engineering methodologies to investigate, if any available methods support a domain expert centered approach in the context of electronic service provisioning in public administration.

Considering the resulting requirements of the E-Government domain identified in the beginning of this chapter, Stadlhofer et al. came to the conclusion that none of the analyzed methodologies is fully capable to serve as domain expert centered ontology engineering methodology in the context of PA. As a result, only one of the tested methods named “Integrated Modeling Methodology” technically addresses all methodological requirements in an acceptable way, but this method was developed for a different domain, namely organizational learning, which means that it’s direct exploitation for the E-Government domain is very difficult. But, the authors of the methodological comparison analysis mention that aspects and general guidelines of this and other methods can contribute to a future methodology in this field [3].

IV. ODEG MODELLING PROCESS

Basically, there are different roles involved in the ontology engineering process. At least, there are two different individuals, namely domain and technical experts. The focus lies on these two roles although there could be more people involved, for example knowledge engineers or ontology users.

1) Domain expert: Domain experts or, in case of the E-Government domain, legal experts possess the required knowledge about the targeting problem domain. The goal is to extract this knowledge, abstract it and transform it into an ontology. This role is necessary and acts as a key role in the ontology engineering process.

2) Technical expert: Technical experts have the required skills to model, design, verify and implement ontologies. Mostly, they are experts in developing software because ontology engineering is a software engineering-oriented process. Furthermore, technical experts possess knowledge about a specific ontology modelling language like WSML or OWL which enables them to build and model ontologies.

The problem here is that both described roles are mandatory to succeed in building usable ontologies. Basically, there are different solutions available to overcome this particular problem. One possibility could be to convert technical experts into domain experts. But, sadly, this intention is impossible to realize. The same applies to the intention to convert domain experts into technical experts: The effort simply would be too expensive and inefficient which leads to the conclusion that another solution is needed to overcome the primary problem.

Therefore, adequate tools are required to bridge the gap between technical and domain experts. The primary goal here is to hide the used ontology language which enables domain experts to use these tools. Furthermore, an easy to use graphical user interface has to be used which supports users on the process level to ease the general ontology engineering process.

ROCKET [4] represents a pilot project to meet the mentioned requirements. This ontology creation tool focuses on enabling domain experts of the Public Administration domain to autonomously develop, build and implement ontologies without the help of technical experts. As a result, these developed E-Government services should be directly executed by the SeGoF web application.

A. ODEG modelling process

Basically, the ODEG modelling process is divided into different phases. Figure 1 gives an overview of these phases and describes them in more detail. It is important to mention, that these process steps are not strictly aligned. As depicted by the life cycle, different process steps can be performed individually. As shown in the middle of the figure, maintenance is also a relevant step which implies that certain actions have to be repeated to achieve acceptable, correct and useful results concerning the created ontology. Maintenance also implies that it may be important to extend the expressiveness of the actual domain, for example, by creating additional sub concepts and respective axioms, or in other words, to refine and extend the modelled domain. In addition, it is important to mention that this life cycle is only a recommendation for further studies which explicitly have to investigate the ODEG modelling process.

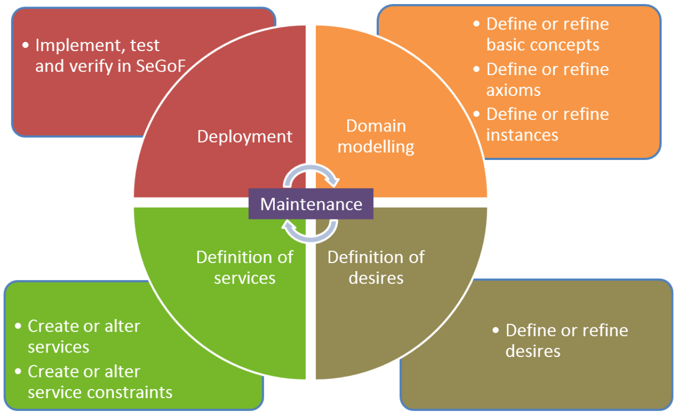

• Implement, test and verify in SeGoF
Deployment
Domain modelling
• Define or refine basic concepts
• Define or refine axioms
• Define or refine instances
Maintenance
Definition of services
Definition of desires
• Create or alter services
• Create or alter service constraints
• Define or refine desires

Figure 1: ODEG modelling process

1) Domain modelling: As mentioned by Stadlhofer et al. [3], service discovery from a citizens point of view should start with selecting the appropriate life situation which are expressed in ODEG by the concept PADomain. For every created domain in the system, a new instance of this concept has be to be defined. The created instance is located in the Domains.wsml file which can be found in the segof/domains folder. Moreover, it is possible to define a list of additional general-purpose ontologies which are relevant for the respective domain [3].

As a next step, it is necessary to model the new created domain. This implies the definition of new concepts, axioms and instances which express the abstracted domain of interest. The following components can be found in the WSML file located in the domain folder in the respective PADomain folder hierarchy.

Definition of concepts: The basic components of every ontology to describe the targeting domain are concepts. Depending on the desired level of detail concerning a domain of interest, several concepts may exist.

Definition of axioms: Furthermore, it may be important to refine the created concepts or to create specific constraints. Therefore, Axioms have to be created which are based on logic programming rules. Of course, it is possible that several axioms may exist in the domain.

Definition of instances: Additionally, it may be relevant to create instances of certain concepts. These instances are also located in the domain WSML file and include concrete values of certain attributes.

2) Definition of desires: After selecting the appropriate life situation, a citizen has to choose one concrete desire or goal he or she wants to reach. For every existing PA domain, it is possible that several desires exist. The isRelatedToConcept attribute expresses the relationship to one or more concepts of the domain and marks the entry point in the ontology.

As mentioned by Stadlhofer et al. [3], in the resulting user interface the user would have the possibility to replace the related concepts in the desire definition by concrete ones. After defining such a concrete desire, an appropriate public service can be discovered for this specific situation.

3) Definition of services: Another important step of the ODEG modelling process is to define specific public web services. Therefore, every semantic service description is split into two different parts. This includes an instance of the geaGrazConstraintPublicService and a corresponding Web Service Modelling Ontology (WSMO) web service. The GEA part includes the description of the relationship to one or more desires and specific constraints that have to be met. By contrast, the WSMO part describes the required input and preconditions [3].

Furthermore, it is possible to create specific constraints which have to be met.

4) Deployment: As the final step in the ODEG modelling process, it is important to implement, test and verify the modelled domain in the SeGoF web application. Therefore, the modelled domain has to be implemented into the respective folder of the SeGoF application, as well as specific entries have to be added to register the new domain. After verifying the created domain, it may be important to refine or extend the existing domain.

V. Human-Centered Ontology Engineering with ROCKET

Basically, ROCKET offers several features concerning the modelling of ontologies. The most important characteristics are going to be described in the following chapter. For more information on ROCKET, please see [4].

A. Axiom editor (sub-concept by constraint)

Creating different concepts which have the same super concept is a common step. That implies that the reasoner has to decide either to take the right or the left path through the ontology. Therefore, axioms are required to accomplish that goal and to tell the reasoner which path to choose for a specific situation. In this concrete example depicted in Figure 2, the super concept “PossiblePupil” holds two attributes, namely “age” and “name”. If a person is 14 years old or younger, this person will become a “RequiredSchoolPupil”. If the person is 15 years old or older, this person will become a “NotRequiredSchool”. It is important to mention that these conditions are implemented in respective axioms. Basically, the described scenario is very common, which implies that it would make sense to combine the action of creating concepts and axioms in one step.

Basically, the primary goal of the new “Sub concept by constraint” feature is that users have the possibility to create a new sub concept of an existing super concept and additionally are able to create a respective axiom. Depending on the selected super concept, the available attributes from the super concept should be visible which can be used to create reasonable constraints.

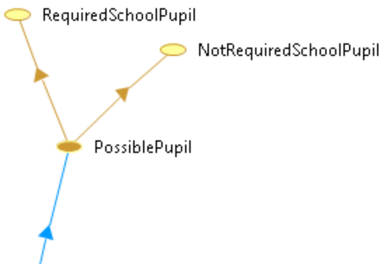
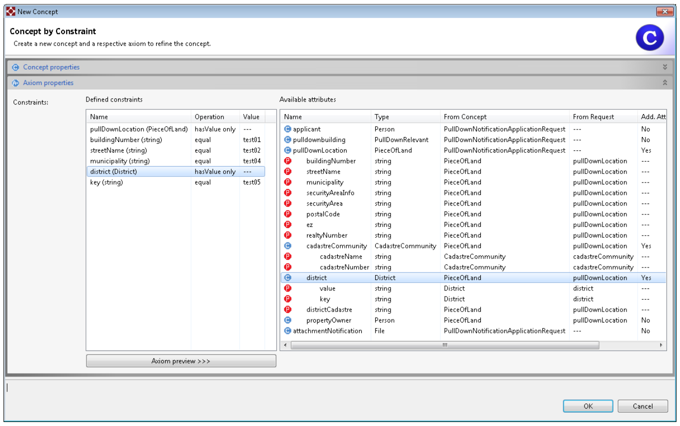


Figure 2: Two different concepts and their super concept

There are two entries in the “Add Entity” context menu in the WSML visualizer when selecting a concept node: the “Sub Concept by Constraint” and “Axiom” option. Selecting the first options allows users to create a sub concept while creating a respective axiom at the same time. As mentioned before, axioms allow to refine concepts and to add specific constraints. Selecting the “Axiom” option allows users, as the name already indicates, to create and model an axiom only. Furthermore, when selecting the root ontology node, the available options differentiate compared to the options. Doing so allows the user to select the “Concept by Constraint” option which creates a normal concept and an additional axiom. In fact, the resulting dialog remains the same.



Concept by Constraint

Create a new concept and a respective axiom to refine the concept.

Constraints:

Defined constraints

Name	Operation	Value
pullDownLocation (PieceOfLand)	hasValue only	---
buildingNumber (string)	equal	test01
streetName (string)	equal	test02
municipality (string)	equal	test04
district (District)	hasValue only	---
key (string)	equal	test05

Available attributes

Name	Type	From Concept	From Request	Add. Att
applicant	Person	PullDownNotificationApplicationRequest	---	No
pulldownbuilding	PullDownRelevant	PullDownNotificationApplicationRequest	---	No
pullDownLocation	PieceOfLand	PullDownNotificationApplicationRequest	---	Yes
buildingNumber	string	PieceOfLand	pullDownLocation	---
streetName	string	PieceOfLand	pullDownLocation	---
municipality	string	PieceOfLand	pullDownLocation	---
securityAreaInfo	string	PieceOfLand	pullDownLocation	---
securityArea	string	PieceOfLand	pullDownLocation	---
postalCode	string	PieceOfLand	pullDownLocation	---
ez	string	PieceOfLand	pullDownLocation	---
realtyNumber	string	PieceOfLand	pullDownLocation	---
cadastreCommunity	CadastreCommunity	PieceOfLand	pullDownLocation	Yes
cadastreName	string	CadastreCommunity	cadastreCommunity	---
cadastreNumber	string	CadastreCommunity	cadastreCommunity	---
district	District	PieceOfLand	pullDownLocation	Yes
value	string	District	district	---
key	string	District	district	---
districtCadastre	string	PieceOfLand	pullDownLocation	---
propertyOwner	Person	PieceOfLand	pullDownLocation	No
attachmentNotification	File	PullDownNotificationApplicationRequest	---	No

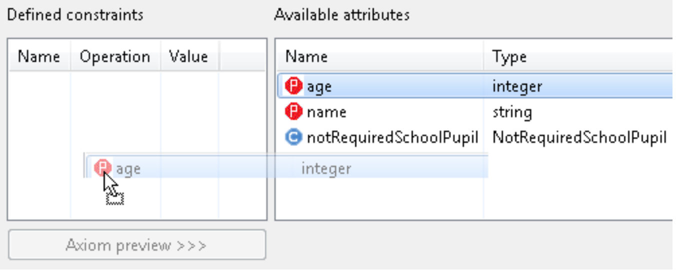
Figure 3: “Sub concept by constraint” dialog

Figure 3 shows the implemented dialog. Basically, the dialog includes basic components like in the normal “New Concept” dialog. It is important to mention that the dialog uses the full size of the display. That means that depending on the size of the ROCKET program, the dialog scales itself to guarantee a better user experience. Furthermore, it is possible to hide all elements which are related to the concept properties. Therefore, users have the possibility to click on the top bar to extend or to hide related user interface elements.

First of all, users have to type in a valid identifier or name for the new sub concept. This name is also used for the name of the respective axiom. Concerning this name, the identifier will be modified by adding the string “Definition”. For example, when users want to create a sub concept named “PossiblePupil”, the respective axiom name would be “PossiblePupilDefinition”. It is also possible to assign specific internationalized human readable descriptions which are important for the SeGoF web application.

Like in the normal “New Concept” dialog, it is possible to add certain annotations and super concepts which influence the resulting concept. Additionally, it is possible to select the “Add relevant imported ontologies” options.

Basically, an axiom consists of different constraints which can be modelled with the help of different gestures. This includes for example the use of drag and drop gestures as demonstrated in Figure 4. Alternatively, another option is to double click on the respective attribute.



Defined constraints

Name	Operation	Value

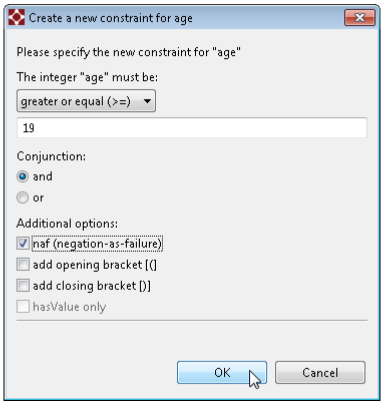
Available attributes

Name	Type
P age	integer
P name	string
C notRequiredSchoolPupil	NotRequiredSchoolPupil

P age integer

Figure 4: Creating a constraint while using the drag and drop gesture

As shown in Figure 4, there are different icons displayed for available attributes. The red “P” indicates that the attribute is a primitive data type, while the blue “C” indicates that the respective attribute is another concept which possibly holds additional attributes. To browse through these attributes of other concepts, users have the possibility explore them by double clicking on a concept. As a consequence, additional attributes will be added under the respective concept.



Create a new constraint for age

Please specify the new constraint for "age"

The integer "age" must be:

greater or equal (>=)

19

Conjunction:

● and

○ or

Additional options:

☑ naf (negation-as-failure)

□ add opening bracket [(]

□ add closing bracket [)]

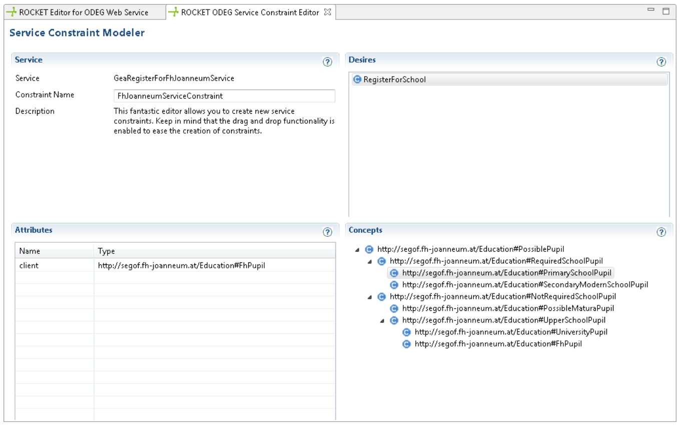
□ hasValue only

Figure 5: Dialog for creating a constraint for the type integer

It is important to mention that depending on the selected type of the attribute, a specific dialog will show up. As shown in Figure 5, the new dialog offers the possibility of adding additional options to the new constraint. In case of an attribute of type integer, the user can choose between different operations like greater, smaller, greater or equal, etc. Of course, a specific number can be added which fulfils the constraint. Furthermore, the desired conjunction can be chosen. In the additional options, users have the possibility of adding the negation keyword “naf”, adding opening and closing brackets and selecting the option “hasValue only”.

B. Service constraint modeller

The ROCKET editor for ODEG web service focuses on the management of available services in the domain. On the left side, all available services will be displayed. By selecting another service, all respective parameters can be checked and altered. This includes available service constraints, related desires, service implementations, related service requests and the name of the service. Furthermore, the user can determine if the service should be an information service, which means that as a result, the SeGoF web application provides a document (e.g., a .pdf file) which includes valuable information for the citizen.



ROCKET Editor for ODEG Web Service
ROCKET ODEG Service Constraint Editor

Service Constraint Modeler

Service

Service: GeaRegisterForFhJoanneumService

Constraint Name: FhJoanneumServiceConstraint

Description: This fantastic editor allows you to create new service constraints. Keep in mind that the drag and drop functionality is enabled to ease the creation of constraints.

Desires

RegisterForSchool

Attributes

Name	Type
client	http://segof.fh-joanneum.at/Education#FhPupil

Concepts

- http://segof.fh-joanneum.at/Education#PossiblePupil
  - http://segof.fh-joanneum.at/Education#RequiredSchoolPupil
    - http://segof.fh-joanneum.at/Education#PrimarySchoolPupil
    - http://segof.fh-joanneum.at/Education#SecondaryModernSchoolPupil
  - http://segof.fh-joanneum.at/Education#NotRequiredSchoolPupil
    - http://segof.fh-joanneum.at/Education#PossibleMaturaPupil
    - http://segof.fh-joanneum.at/Education#UpperSchoolPupil
      - http://segof.fh-joanneum.at/Education#UniversityPupil
      - http://segof.fh-joanneum.at/Education#FhPupil

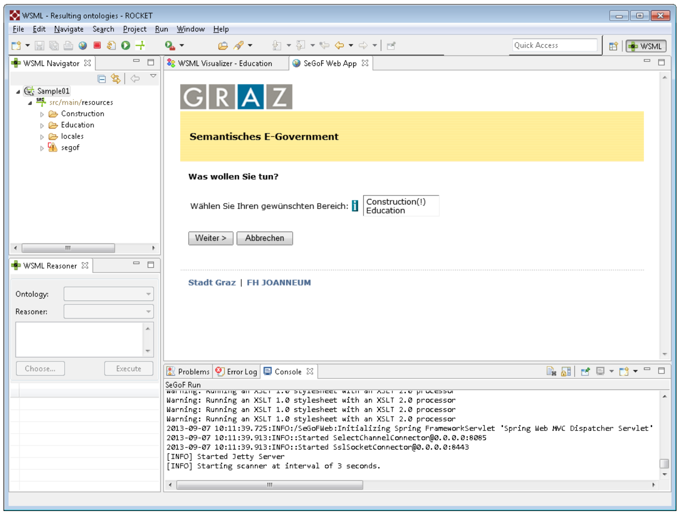
Figure 6: Service constraint modeller

Another important part of the web service editor is the ODEG service constraint modelling editor which pops up by selecting the edit or create button after right clicking into the area of the service constraints. As depicted in Figure 6, users have the possibility to create specific constraints for the respective service. Depending on the selected desire, different concepts will be displayed as a tree. By using intuitive drag and drop gestures, it is possible to select a desired concept and drop it in the attributes area to create an additional attribute. Therefore, the user has to provide a new name. After creating a new or editing an existing constraint, users have to save the changes by pressing CTRL + S. In the background, the new or changed service constraint will be stored in the respective domains file as an instance of type geaGraz#ServiceConstraint including the created attributes.

C. Automatic implementation of ontologies in SeGoF

Another feature is called “run button”. As a developed use case confirmed, the test and verification steps of the ontology in the SeGoF web application are rather complicated and not supported by the tool ROCKET. As a result, users have to manually add the generated ontology and the segof wsml files in the respective folder in SeGoF, build the SeGoFOntologies project and start the jetty web server via the console. Since this is not a human-centered approach, additional features have to be added to give users the possibility of implementing, testing and verifying the created ontology directly in ROCKET. Therefore, a new button has to be implemented in the tool which executes the described steps of deploying the ontology in SeGoF automatically. Besides reducing the level of difficulty of the steps which have to be executed manually, users would have the possibility of verifying the ontology very quickly.

1) Main run button: The main run button located on the right side of the four new buttons acts as the primary button to initiate the start of the SeGoF web application. This button has to be executed before using the others. First of all, when pressing this button, ROCKET copies the required SeGoF run files from its sources into the actual workspace. This includes a folder holding the maven binaries, the SeGoFOntologies project and the SeGoFWeb project and other relevant projects from the SeGoF web application, respectively in separate folders. After copying the new folders, the respective WSML files (depending on the selected project in ROCKET) will be implemented in the SeGoFOntologies project and the preconfigured and pre-built SeGoFWeb.war and other required files will be installed in the local maven repository. As a next step, this project will be built using the implemented maven sources. Depending on the operating system of the host system of ROCKET, a specific maven run file and a proper command will be chosen to accomplish this task. That implies that maven is not a prerequisite when users are executing the run button, which is a big advantage. Furthermore, the integrated jetty web server will be started and the internal browser of ROCKET will be opened displaying the correct page with the address “localhost:8080/SeGoFWeb” as shown in Figure 7. Now, users have the possibility of verifying and testing the modelled ontology instantly.



Semantisches E-Government

Was wollen Sie tun?

Wählen Sie Ihren gewünschten Bereich: Construction(!) Education

Weiter > Abbrechen

Ontology:

Reasoner:

```
Warning: Running an XSLT 1.0 stylesheet with an XSLT 2.0 processor
Warning: Running an XSLT 1.0 stylesheet with an XSLT 2.0 processor
Warning: Running an XSLT 1.0 stylesheet with an XSLT 2.0 processor
Warning: Running an XSLT 1.0 stylesheet with an XSLT 2.0 processor
2013-09-07 10:11:39.725:INFO:/SeGoFWeb:Initializing Spring FrameworkServlet 'Spring Web MVC Dispatcher Servlet'
2013-09-07 10:11:39.913:INFO::Started SelectChannelConnector@0.0.0.0:8085
2013-09-07 10:11:39.913:INFO::Started SslSocketConnector@0.0.0.0:8443
[INFO] Started Jetty Server
[INFO] Starting scanner at interval of 3 seconds.
```

Figure 7: Internal browser in ROCKET

2) Refresh button: After executing the main run button for the first time, the jetty web server is up and running. When users modify a respective ontology, they have the possibility to execute the refresh button so that only the new WSML files get copied and the project SeGoFOntologies gets built. The running jetty web server detects the modified jar file from the SeGoFOntologies projects and restarts itself automatically. Of course, it is possible to re-execute the main run button, but the advantage of the refresh button is that it finishes much quicker.

3) Stop button: As the name of the button already indicates, the stop button stops the running jetty web server and closes the internal browser view automatically. This, for example, is useful when quitting ROCKET to close all remaining processes. As usual, the status of this process can be checked in the console view.

4) Open browser button: This button allows users to re-open the internal browser view if the Jetty web server is running. If the server is not running, a respective error message will be displayed telling users that SeGoF is not running. Furthermore, this button refreshes the actual address of the browser to the default address. This is useful when testing different PA domains to return to the initial web page.

VI. Conclusion

First of all, the illustration of the ODEG modelling process is an important step toward a well-defined and structured process concerning the ontology building process in ROCKET. While the depicted life cycle is only a recommendation, it can be seen as an important input for further studies in this field. The ontology creation tool ROCKET offers several specific wizards and editors which allow users to build and model a specific ontology in the field of E-Government which can be used by the SeGoF web application as an input to automatically generate E-Government forms to ultimately invoke a certain service. The top-level goal of ROCKET is to empower domain or legal experts so that they are able to build ontologies autonomously. Furthermore, ROCKET offers an easy to use graphical user interface which guides users through the ODEG modelling process by pursuing a human-centered ontology engineering approach. Additionally, tools like the WSML Visualizer help users understand the modelled ontology more easily. To conclude, it is important to mention that future work has to be focused on conducting usability tests to improve the overall usage of the tool. Consequently, the ontology engineering methodology ODEG has to be further developed to achieve a well-defined and documented process. With the help of SeGoF and ROCKET, the efficiency of public offices concerning the offering of public services can be increased significantly. Because of the fact that legal experts would design and model ontologies autonomously which then will be used as an input for the SeGoF web application, public services could be published immediately.

References

[1] Peter Salhofer and Bernd Stadlhofer, “Semantic MDA for E-Government Service Development”, hicss, pp. 2189-2198, 2012 45th Hawaii International Conference on System Sciences, 2012, http://doi.ieeecomputersociety.org/10.1109/HICSS.2012.524, [retrieved: 10, 2013].

[2] Peter Salhofer, Bernd Stadlhofer, and Gerald Tretter, “Ontology Driven E-Government”, in Politics, Democracy and E-Government: Participation and Service Delivery (Reddick, Ch., editor), Information Science Reference, April 2010, pp. 383-401.

[3] Bernd Stadlhofer, Peter Salhofer, and Augustin Durlacher, “An Overview of Ontology Engineering Methodologies in the Context of Public Administration”, p. 7, 2012.

[4] Bernd Stadlhofer, Peter Salhofer, Augustin Durlacher, and Martin Zierler, “ROCKET - Rich Ontology Creation Kit for E-Government Transition”, in Electronic Government and Electronic Participation, Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and IFIP ePart, Kristiansand, Norway, September 3-6, 2012, Trauner Verlag, pp. 106-114.

Proposal on operator-assisted E-Government Systems

Yoshihiro Uda, Kazuhiro Yoshida and Yoshitoshi Murata
Graduate School of Software and Information Science
Iwate Prefectural University
Iwate, Japan
e-mail: g236i002@s.iwate-pu.ac.jp, kazuhiro.iwk@gmail.com, y-murata@iwate-pu.ac.jp

Abstract—**Japan is ranked 18th in the world in the 2012 United Nation's e-Government database. People experience poor system usability due to bureaucratic wording (jargon) and non-universal interfaces. For a better e-Government system experience, we propose an operator-assisted e-Government system. In this system, operators at a call center assist applicants by giving application process guidance as well as taking over keyboard operation for people with low IT literacy. Jargon is a major obstacle in Web site usability; therefore, we propose an analysis tool for evaluating current Web sites based on a phrase difficulty index. Evaluation experiments on a prototype system suggested that operator-assisted application shortened the process time by 20% compared to conventional solo application. Also, errors were negligible for operator-assisted application. Calculated process times obtained from the analysis tool showed good agreement with the experimental results. The proposed e-Government system will greatly help to accelerate system usage by the elderly and people with low IT literacy.**

Keywords-e-Government; call center; Web site usability; jargon; operator-assisted application.

I. Introduction

The Japanese-Government has promoted an e-Government system since 2006. However, the acceptance of the system is not as high as expected. According to the United Nation's e-Government database in 2012, Japan ranked 18th in the world, while the Republic of Korea has remained on top for years [1]. Many studies on e-Government system usability were carried out and major issues were pointed out such as bureaucrat wording (jargon) and the lack of uniform interfaces among systems. Instead of fully redesigning the current e-Government systems, usability improvement of current system is desired in view of economy and speed.

We propose an e-Government system with a call center operator assistance for applicants to improve the user interface. The operator talks with applicants over the phone to help with the application process and takes over keyboard operation for applicants who are not familiar with Personal Computers (PCs) and the Internet. The proposed system's effectiveness was examined through model system experiments to measure the process time and errors in the application contents.

We use our proposed phrase difficulty rank evaluation tool for usability analysis of current Web sites. The evaluation tool is useful to determine the possibility of improving usability by adding the call center functionality for current e-Government systems.

Section 2 describes related work on e-Government systems and their usability issues. Objectives of this study are discussed in Section 3, and the model system experiments are explained in Section 4. The experimental results are given in Section 5, followed by the conclusions.

II. Related work on e-Government system usability issues

Web site usability issues have been discussed for years [2], [3]. At the beginning stage of the e-Government system, both governments and citizens expected the systems would be quickly and widely accepted. However, the adaption rate of e-Government systems is slower than e-commerce and other Web-site-based systems.

Fuchs clearly pointed out substantial differences between e-commerce and e-Government systems, e.g., no competition for the same services, lack of uniform outlooks, and subdivided territorial levels due to broad public administration scopes [4]. These findings explain why current e-Government systems' one-stop interfaces cannot be used for different applications (tax payment, passport application, etc.) and why system usability is usually lower than that of e-commerce systems [5-8].

Wording (jargon and technical terms) is a significant indication of low usability of e-Government Web sites [8]. Applicants are forced to take time to learn the jargon on the e-Government Web site pages. When jargon must be used in Web pages, proper explanation should be included. Also, application process guidance should be given on the Web page for applicants. We found that some e-Government Web sites have links to operation manuals, but most of applicants would not willingly spend time to either read the huge manuals in detail or even notice the attachments.

Gauvin et al. found that age is a markedly higher demographic determinant of Internet usage than education, income, gender, and urbanity [10]. Thus, assisting the elderly with the Internet and e-Government system operations has become an important issue for governments to better serve their citizens in view of e-inclusion [11], [12], [13]. Kim reported that "mass digital literacy campaigns" for several tens of millions of elderly, government officials, and housewives were carried out as Information Technology (IT) education programs in Korea, which has been consistently at the top of the e-Government system usability ranking. This is one of the key success factors for Korean e-Government systems [14], but such an education system is not always applicable to the large population of senior people like in Japan. Moreover, Internet access platform expands from the fixed line communication by PCs to smart-phones and tablets. Preparing education programs which cover all the different access platforms takes time and may not be ready when the evolution occurs on IT networks. This paper proposes a new user assistance system, which has better applicability than the user education.

III. PROPOSED E-GOVERNMENT SYSTEM

3.1 A proposed system function

Senior citizens and other people with low IT literacy require proper assistance to use an e-Government system. Therefore, call centers have been used as help desks to assist applicants with the e-Government system [15], [16]. Call center operators assist applicants by helping with the application process and answering applicants' questions on jargon. The call center system offers the flexible service by training operators for the access platform evolution. On the other hand, data protection and applicants' privacy protects are remaining issues for the call center system [13].

Our proposed system extends the call center operator function from verbally assisting applicants to taking over keyboard operation for applicants [17], [18]. This would greatly reduce the burden on low-IT-literacy applicants. This system is expected to reduce the application process time as well as minimize the operation and application errors.

As discussed in the previous section, e-Government systems which contain a large amount of jargon result in poor Web site usability and high possibility of making errors in the application process. Solo application process time may be longer through difficult Web sites than through operator-assisted application. Also, fewer errors in operator-assisted application are expected than on solo application. From this viewpoint, we believe that e-Government Web site usability can be measured based on process time and application error rates. These assumptions were verified through experiments and explained in the following Section.

We also propose a numerical analysis tool in terms of jargon difficulty in usability evaluation of current Web site. The jargon difficulty index definitions are given for the major phrases used on the Web pages. The difficulty levels are then applied to process time calculations for applications with and without operator assistance. By using the analyzed results (expected times and error rates), e-Government system owners can predict the call center effectiveness for current e-Government systems.

3.2 The system configuration

Operators located at call centers for e-Government systems talk with applicants over the phone (Fig. 1). During the application process, the applicant and operator share the Web pages of the application system through their respective PC displays (Fig. 2). The page sharing system is implemented by the following technologies:

a. Applicant identification: The applicants are given separate identification numbers (e.g., phone numbers) to correspond with the operator over the phone and Web pages.

b. Web page sharing between the applicant and the operator: Two Web page sets are prepared from the current e-Government system database: (a) Web pages for applicants and (b) those for operators. During the operator-assisted application process, the operator works on the PC keyboard and fills in the application form on the operator Web pages based on the conversation with the applicant. The application contents are stored in the database at the call center.

c. Confirmation of application contents: When the operator finishes keyboard work, the Web pages are displayed on the applicant's PC so that the applicant can check if the contents are the same as what the applicant gave to the operator. After content confirmation, the applicant clicks on the register button on the Web page and finalizes the application form to be sent from the call center database to the e-Government system.

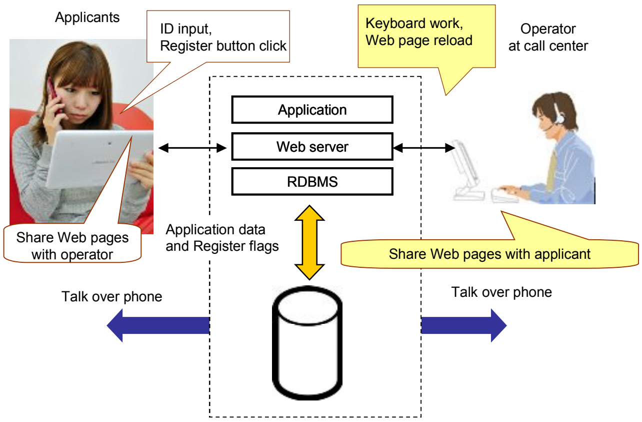
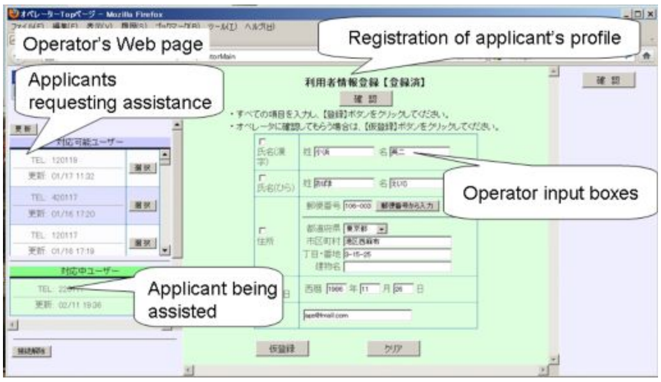


Figure 1. Proposed configuration for operator-assisted e-Government system.



利用者情報登録【登録済】

確認

・すべての項目を入力し、【登録】ボタンをクリックしてください。
・オペレータに確認してもらう場合は、【仮登録】ボタンをクリックしてください。

対応可能ユーザー
TEL: 120119 更新: 01/17 11:32 選択
TEL: 420117 更新: 01/16 17:20 選択
TEL: 120117 更新: 01/16 17:19 選択

対応中ユーザー
TEL: 22… 更新: 02/11 19:36

氏名(漢字) 姓 名
氏名(ひら) 姓 名
郵便番号 106-003 郵便番号から入力
住所 都道府県 東京都
市区町村 港区西麻布
丁目・番地 3-15-25
建物名
西暦 1966 年 11 月 26 日

仮登録 クリア 接続解除

Figure 2. Example of operator's page on operator's display.

3.3 An evaluation tool for Web site usability

There are many materials to determine the difficulty level of kanji (Chinese characters used in Japanese language), mainly prepared for non-Japanese speakers. Basic Japanese words are also classified for Japanese students and foreigners [19]. However, most of the jargon found in e-Government Web sites are not included in the current basic word classifications and no difficulty levels are available. E-Government jargon requires a much higher reading level than for students because they are not common in text books, newspapers, and magazines.

We propose an evaluation tool to determine the phrase difficulty rank for jargon appearing in e-Government Web sites. The difficulty rank definition is given by assigning unique difficulty indexes as extended ranks in the Balanced Corpus of Contemporary Written Japanese (BCCWJ) [20]. The BCCWJ covers a wide range of popular phrases found in books, magazines, newspapers, and Web sites.

The index assignments are ranked as follows.

Rank 1: Phrases found in "Kanji (Chinese characters) 2100 [19]." This rank corresponds to the basic words at the reading level of junior high school students.

Rank 2: Phrases not listed in "Kanji (Chinese characters) 2100," but have 100 or more search results in the BCCWJ.

Rank 3: Phrases which have 10 to 99 search results in the BCCWJ.

Rank 4: Phrases which have less than 9 search results in the BCCWJ or only some of the words in the phrases are found in the BCCWJ.

Analysis of Web site usability is carried out as follows.

Step 1: List all the phrases used in an e-Government Web site.

Step 2: Assign phrase ranks to the listed phrases per the above-mentioned indexes.

Step 3: Obtain a summary of phrase ranks, which appear in a particular application theme (described below) before filling in one of the input boxes of the Web page.

The phrase ranks are also applied to the expected process time calculations by solo and operator-assisted applications, as described in Section V-3.

IV. EVALUATION EXPERIMENTS

4.1 Application themes

Evaluation experiments were carried out to confirm the effectiveness of the proposed system for improving system usability, as discussed in Sections 2 and 3. The measured parameters for usability comparison between current application systems and the proposed one were processing time and the number of application errors.

Based on current e-Government and e-application systems, six application themes were prepared on a Web server as a set of Web pages and databases. The themes were designed from simple to complicated processes as well as those which require good understanding of the process and jargon (Table 1). The design concepts for the themes are listed below.

Theme A: Registration of applicant profile; Applicant's name, address, etc. This theme focuses on the correct inputs for the application form.

Theme B: Certificate of residence: Applicants are guided to register their new bike. One of the requested documents is the certificate of residence. This theme examines if the applicant can choose the proper document required for bike registration.

Theme C: Family register certificate: Applicants are guided to change the legal domicile for their new passport.

The theme examines if the applicant does not mix the old and new domiciles, as well as current living address (note: in Japan, the legal domicile and the living address may not be the same).

TABLE I. NUMBER OF PHRASES IN APPLICATION THEMES CLASSIFIED BY PHRASE RANK.

Rank	A Regis-tration	B Resi-dence certifi-cate	C Family Regis-ter	D Confer-ence	E In-come tax	F Tax certifi-cate
1	5	0	0	0	6	4
2	2	3	2	2	7	9
3	0	2	2	8	11	13
4	0	1	0	5	11	13

Theme D: Technical conference registration: Applicants are requested to fill in the registration form for a technical conference. The theme is prepared to examine if the correct options have been selected and calculate the registration fee under given conditions (member discount, etc.).

Theme E: Income tax calculation: A simplified tax calculation system is provided. Applicants are requested to input the total income as well as deductions of life insurance, social insurance, and medical expense. The theme examines if the applicant can understand the deduction system described with a large amount of jargon and make correct calculations for the related deduction items.

Theme F: Tax payment certificate: The applicants need the tax payment certificate for housing loan refinancing. The certificate application form is complicated and difficult to understand due to the jargon. The theme design concept is similar to Theme E, testing information access and correct calculations.

4.2 The experiment design

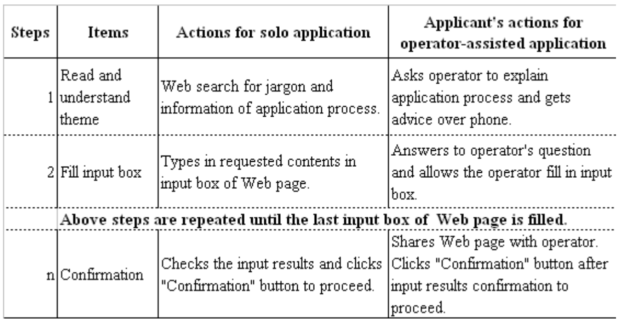
Each test participant was given a separate identification number. The test participants were divided into either a solo application group or operator-assisted application group. The solo application group simulated conventional application systems. The operator-assisted application group was established to confirm the advantages of the proposed system.

The test participant and operator had their own PCs and displays, but they could not look at the other's. The applicant's profile (name, address, birth date, etc.) was given as a fictitious identity and was commonly applied to all the test participants.

4.3 The experiment process

Applicant action steps are summarized in Table 2. The solo application group tried to complete all the themes themselves. A test participant read a theme and understood what information and actions were necessary to complete the application. When the test participant could not understand

TABLE II. APPLICANT ACTION STEPS.



Steps	Items	Actions for solo application	Applicant's actions for operator-assisted application
1	Read and understand theme	Web search for jargon and information of application process.	Asks operator to explain application process and gets advice over phone.
2	Fill input box	Types in requested contents in input box of Web page.	Answers to operator's question and allows the operator fill in input box.
	Above steps are repeated until the last input box of Web page is filled.		
n	Confirmation	Checks the input results and clicks "Confirmation" button to proceed.	Shares Web page with operator. Clicks "Confirmation" button after input results confirmation to proceed.

the technical terms and jargon in the theme expression, he/she had to use Internet search engines for guidance and explanations and process the application the Web pages.

A test participant in the operator-assisted application group directly talked with the operator (one of the authors) instead of making a phone call. After the test participant chose a theme, he/she asked the operator for guidance. With the operator's guidance, the test participant gave information to the operator. The operator looked at the application Web page and worked on the keyboard. After finishing the input process, the operator told the test participant to update the Web page so that the test participant could confirm the given information correctly appeared in the application form. When the test participant confirmed the application form, he/she clicked on the "register" button on the Web page and the application was completed.

V. EVALUATION OF EXPERIMENT RESULTS

5.1 Test participants

Thirty-seven participants (20 students and 17 office workers) were divided into 27 solo applicants and 10 operator-assisted applicants. The operator-assisted group was smaller than the solo-application group, because the preliminary experiments showed highly consistent results for both the process time and errors in the operator-assisted applications. The participant profiles were classified by generation and years of PC experience (Fig. 3).

5.2 Experimental results

Both time and error comparisons suggest the effectiveness of operator assistance during the application process.

Figure 4 shows the experimental results of the average processing times for both solo and operator-assisted applications. Solo application took 20% more time to finish the latter three themes (D, E and F) than operator-assisted one. Error rates are also compared between solo and operator-assisted applications (Fig. 5). Operator-assisted application significantly reduced errors compared to solo

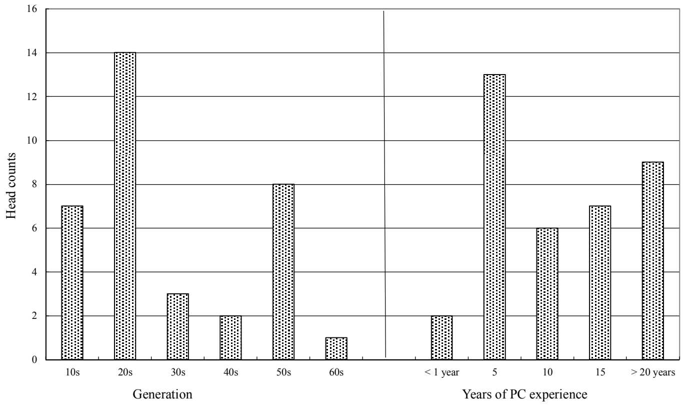


Figure 3. Test participant profiles (generation and years of PC experience).

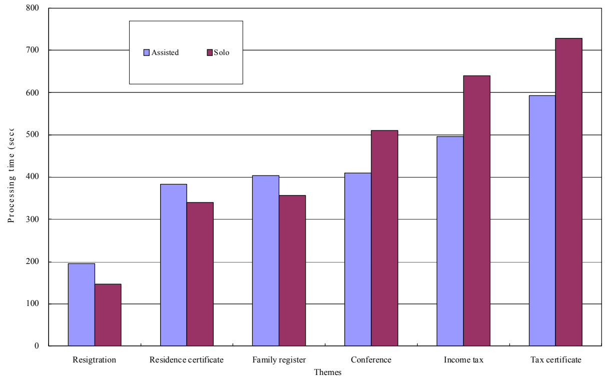


Figure 4. Experimental results of average processing times for operator-assisted and solo applications.

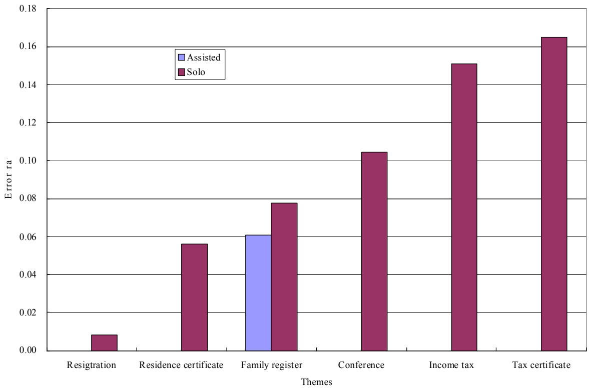


Figure 5. Experimental results of error rates for operator-assisted and solo applications.

application except the theme C, on which some participants confused the living address with the legal domicile and gave wrong information to the operator.

5.3 Experimental result analyses

Process time calculation was carried out using the proposed analysis tool for each experiment theme. Table 4 shows part of the analysis table for Theme E (Income tax calculation). In this example, the first input box is the medical expense tax deduction amount. Prior to filling in this box, the applicant has to understand the meaning of jargon such as "Medical expense tax deduction," "Medical insurance supplementation," and "Hospital expense grant". The phrase ranks for the jargon are given based on the rules explained in Section 3.3. A time factor is then applied to each phrase based on Table 3. The time factors were optimized by fitting the measured times in the experiments to time factor parameter sets. The time factor sum was calculated, and calculated time was obtained for solo application by multiplying the sum and a unit time defined to the input process. Following this process for the entire theme table, the total calculated time was examined. Operator-assisted time is also provided in Table 4.

The differences between solo application and operator-assisted application are:

a. Jargon search and time taken to understand was shorter for operator-assisted application than solo application because the operator could give proper advice to the applicants on the meaning of jargon and operation process.

b. Time to fill in an input box for operator-assisted application was longer than solo application. This was due to the conversation between the applicant and the operator to transfer the necessary information to fill the input box.

c. Verification process was added to the operator-assisted application. After the operator completed filling in the input boxes, he/she had to ask the applicant to check the box contents and to verify the application form. This process is not necessary for solo application.

The calculated times for six themes are shown in Fig. 6 and compared to the experimental results both for solo and operator-assisted applications. The calculated times showed good agreement with the measured results in the experiments. Processing time calculation would be useful to examine current e-Government Web sites in terms of the effectiveness of call center operators to obtain better user interfaces.

VI. CONCLUSION AND FUTURE WORK

We proposed an e-Government system with extended call center functionality. Call center operators talk with applicants over the phone and assist them by helping with the application process and taking over keyboard operations for applicants who are not familiar with PCs and the Internet, such as senior citizens. The proposed system's effectiveness was confirmed through model system experiments by measuring the process time and errors of the application contents for both solo and operator-assisted applications.

The experimental results suggest that the process time for complicated Web sites can be shorten by 20% by operator-assisted application compared to solo application. Also, errors which occurred in solo application were negligible in operator-assisted applications. We also proposed a phrase difficulty rank evaluation tool usability analysis of current Web sites. Analyzed results showed good agreement with the measured processing time for all the themes in the experiments.

These results indicate that the proposed e-Government system will greatly help to accelerate system usage by senior citizens and other people with low IT literacy.

For the future work, we intend to develop the error rate calculation method on the current e-Government Web sites for further site usability analysis. Some other indexes would be considered for the error rate calculation in addition to the proposed phase difficulty rank.

TABLE III. TIME FACTORS VS. PHRASE RANK.

Phrase rank	*Time factor*
1	1
2	1.3
3	1.6
4	1.9

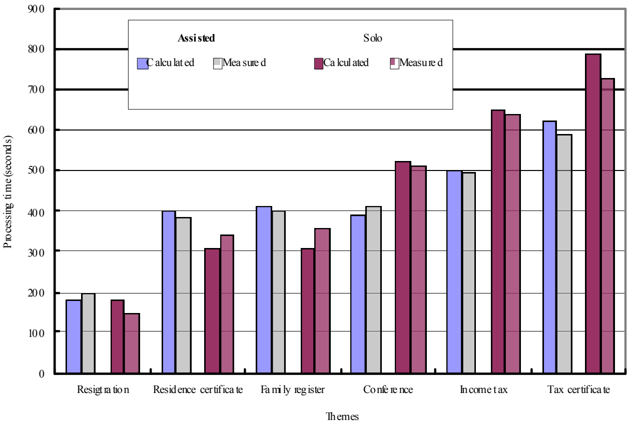


Figure 6. Comparisons of calculated and measured processing times for both solo and operator-assisted applications.

TABLE IV. PART OF ANALYS TABLE FOR THEME E (INCOME TAX CALCULATION)

Application steps	Jargon	Phrase rank	Input items	Time factor	Time factor sum	Solo application calculated time	Operator -assisted application calculated time
Read theme and understand/search	Medical expense tax dedction	2		1.3			
(Note 1)	Medical insurance supplementation	4		1.9			
	Hospital expense grant	4		1.9			
	Major medical expense	2		1.3			
	Family medical expense	3		1.6			
	One-off maternity benefit	3		1.6	9.6	96	30
Fill input box			Medical expense tax deduction amount			10	20
Verification between applicant and operator (Note 2)						—	10
Read theme and understand/search	Social insurance tax deduction	3		1.6			
(Note 1)	National pension	1		1			
	National health insurance	2		1.3			
	Nursing-care insurance	2		1.3			
	Unemployment insurance	3		1.6	6.8	68	30
Fill input box			Social insurance deduction amount			10	20
Verification between applicant and operator (Note 2)						—	10
Note 1: For solo application						Units in seconds	
Note 2: For operator-assisted application							

REFERENCES

[1] United Nations Public Administration Network, “2012 Global E-Government Survey,” 2013 on http://www.unpan.org/egovkb/global_reports/08report.htm [retrieved: January, 2014].

[2] J. Nielsen, “Usability 101: Introduction to Usability,” 2012 on http://www.nngroup.com/articles/usability-101-introduction-to-usability/ [retrieved: January, 2014].

[3] J. Iio and H. Shimizu, “Evaluation improvement method for business system usability,” Research Papers, Mitsubishi Research Institute, vol. 50, pp. 30-53, 2008 (in Japanese).

[4] G. Fuchs, “Lost Youth? Attitudes Towards and Experiences Withe-Government: The Case of Germany University Students,“ Proc. of 12th. European Conference on e-Government, pp. 251-258, 2012.

[5] R. Schwester, “Examining the Barriers to e-Government Adoption,” Leading Issues in e-Government Research, pp. 32-50, Academic Publishing International Ltd., 2011.

[6] D. Evans and D. C. Yen, “E-Government: Evolving relationship of citizens and government, domestic, and international development,” Government Information Quarterly, vol. 23, pp. 207-235, 2006.

[7] S. Elling, L. Lentz, M. De Jong, and H. Bergh, “Measuring the quality of governmental websites in a controlled versus an online setting with the ‘Website Evaluation Questionnaire’,” Government Information Quarterly, vol. 29, pp. 383-393, 2012.

[8] Z. Khabaziyan, H. Teimori, and M. Hekmatpanah, “Planning E-Citizen: A Step toward E-Society”, World Academy of

Science, Engineering and Technology, vol. 59, pp. 2590-2593, 2011.

[9] P. Jaeger and M. Matteson, “e-Government and Technology Acceptance: The Case of the Implementation of Section 508 Guidelines for Websites,” Leading Issues in e-Government Research, pp. 231-252, Academic Publishing International Ltd., 2011.

[10] S. Gauvin, K. Granger, M. Lorthiois, and D. Poulin, “The Shrinking Digital Divide – Determinants and Technological Opportunities,“ Proc. of 12th European Conference on e-Government, Jan. 2012, pp. 259-267.

[11] C. W. Phang, J. Sutanto, A. Kankanhalli, Y. Li, B. C. Y. Tan and H-H Teo, ”Senior citizens’ acceptance of information systems: A study in the context of e-Government services,” IEEE Trans. on Engineering Management, vol. 53, no. 4, pp. 555-569, November, 2006.

[12] T. Molnar, “Best Practices for Improved Usability of e-Government for the Ageing Population, “ Proc. of 12th. European Conference on e-Government, pp. 493-501, 2012.

[13] E. Mordini et al. “Senior citizens and the ethics of e-inclusion,” Springer on http://link.springer.com/article/10.1007%2Fs10676-009-9189-7#page-1, April, 2009 [retrieved: January, 2014].

[14] S. Y. Kim, “Korea ICT/e-Gov History, Best Practices and Lessons,” presented at Georgian Cyber Security and ICT Innovation Conference 2011, Nov. 18, 2011.

[15] A. K. Singh and R. Sahu, “Integrating Internet, telephones, and call centers for delivering better quality e-Governance to all citizens,” Government Information Quarterly, vol. 25, pp. 477-490, 2007.

[16] F. Bao and F. Zhao, “Study on the E-Government Call Center System Based on SOA,” Computer and Information Science, vol. 4, no. 4, pp. 120-122, July, 2011.

[17] Y. Murata, Y. Sato, T. Takayama, and N. Sato, “E-Government System Using an Integrated Call Center System and WWW,” Proc. of the 2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology – vol. 03, pp. 199-202, 2008.

[18] Y. Uda, K. Yoshida, and Y. Murata, “A Proposal and Evaluation of the Operator-assisted E-Government System,” Proc. of Dicomo 2012 (Multimedia, Distributed, Cooperative, and Mobile Symposium), July, 2012, pp. 860-866 (in Japanese).

[19] Y. Tokuhiro, “Kanji (Chinese characters) 2100, Listed according to Frequency and Familiarity,” Sanseido Co. Ltd., 2008 (in Japanese).

[20] Japanese Corpus project, “Shonagon,” 2012 on http://www.kotono.ha.gr.jp/shonagon/ (in Japanese) [retrieved: January, 2014].

Open Government Data

Small Country User's Perspective

Mladen Varga, Katarina Ćurko
Faculty of Economics & Business
University of Zagreb
Zagreb, Croatia
mvarga@efzg.hr, kcurko@efzg.hr

Tomislav Vračić
Ministry of Public Administration
Zagreb, Croatia
tvracic@uprava.hr

***Abstract* -The paper describes how users in a small transitional country perceive open government data. It discusses the objectives of opening government data to the public, considers what end-users require, and investigates impediments to end-user's adoption of open data. The results reveal the following: end-users are generally unprepared to use open data; they have no confidence in the credibility of published data; end users do not differentiate between open data and private data; they are not familiar with the purpose of open data and opportunities arising from using them. Finally, the paper discusses possible government measures to boost open data usage. The following measures are proposed: a single open data portal should be organized; data suppliers should be stimulated to publish, certify and maintain their open data; and end-users should be encouraged to use the data.**

Keywords-open data; open government data

I. Introduction

The concept of open data has existed for some time. It corresponds to open movement, such as open access to scientific information, open source software etc. In this paper, we shall mainly consider government data (GD), also referred to as public sector information (PSI). Government bodies collect, produce, reproduce and disseminate public data in many areas of activity while accomplishing their institutional tasks. These data, such as geographical information, statistics, weather data, transportation data, public health data, etc. are of public interest, belong to the whole community and every citizen is entitled to know and use them. Government data could be opened for re-use by citizens, business and industry, science, media, civil society and others. The benefits of opening government data are numerous, even it is impossible to predict what value it will create in the future [1].

To achieve their full potential, government data must be open. Making data open could enormously increase civil sector engagement. An effective public information system should include a considerable amount of open government data and be equipped with efficient tools for data analysis and visualization.

The paper describes the position and the early experience of an open data initiative in a small transitional country (the Republic of Croatia with about 4 million inhabitants). It discusses the objectives of opening government data to the public, considers what end-users require, investigates impediments to end-user's adoption of open data, and possible government measures to boost open data usage. It is organized as follows. The definition and types of open data are discussed in Section II, end-users' requirements as seen by the average user are described in Section III, the main impediments to citizens' adoption of open government data are considered in Section IV, and possible government measures for boosting the usage of open data are described in Section V and summarized in Section VI. The findings listed correspond to the specific situation of a smaller community, in the grip of recession and not too enthusiastic about opening government data.

II. Definition of Open Data

Formal definitions of open data are relatively new. Open Data Institute [2] defines open data as information that is available for anyone to use, for any purpose, at no cost. OpenDefinition.org [3] defines open data as data that can be freely used, reused and redistributed by anyone.

Private data, i.e., sensitive personal data, cannot be the subject of open data. There is no consensus on what constitutes private data, and the debate on the subject continues.

Two most prominent types of open data are open science data and open government data.

Open science data (OSD) are freely available, allowing any user to read, download, copy, distribute, print, search, index, use by software or use for any other legal purpose. When the data are reproduced or distributed the copyright must be acknowledged, author's control over the integrity of their work must be preserved and the work must be cited. Public availability and reusability of scientific data leads to transparency, fairness and increased quality of science. Open science data are creating value in science itself.

The same is true for open government data (OGD), which we are considering in the paper. Open government data are data produced by government or its bodies, that can be freely used, reused and redistributed by anyone, resulting in a fairer and better government. As discussed in the literature [1], [11], [13], reasons for making data open include: (a) transparency and accountability, (b) innovation and economic development; and (c) inclusion, empowerment and law enforcement.

A. *Transparency and Accountability*

Open data increase transparency. Free access to government data can empower citizens to exercise their democratic rights [11]. Consequently, transparency increases the accountability of government and its bodies. It is reasonable to expect that they will make better decisions in the public interest. The focus is on the political domain. Open data create value in government itself by increasing its efficiency.

B. *Innovation and Economic Development*

Open data may enable innovators to improve services or build new products and services within public or private sector. Open data may shift certain decision making from the state into the market [1]. The key focus is on the economic domain. Open data create value in many ways, for example by helping create new products or services in places where they are missing, including the development of new products built directly on PSI [13].

A type of open data, which may be considered as OGD in a very broad of sense, is open business data (OBD). The key focus is also on the economic domain. The source of data is the business sector. Examples include data collected at the chambers of commerce or trade, statistical or marketing agencies or in corporations that are willing to open their data to general public.

C. *Inclusion, Empowerment and Law Enforcement*

The motivation to open government data is to involve citizens in policing and law enforcement [11]. Open data may remove power imbalances that resulted from asymmetric information, bring new actors in the political debate, especially those with special interests or needs. The key focus is on the social and law domain.

III. USER REQUIREMENTS ON OPEN GOVERNMENT DATA

Who are the typical stakeholders and users of open data? They are not a uniform group of people who share the same urge and interest to access data. In [5] they are classified as public sector, private sector, donors, civil society organizations, academia, civil hackers, and media, depending on their role in open data initiatives. Based on data driven classification [5] they are classified as data producers, data consumers, data intermediaries and data specialists. The Table I presents the different types of stakeholders, based on their expected main roles and tasks.

What do users, i.e., data consumers, expect from open data? They want to have access to (a) all types of useful data, (b) in a single place, (c) that the data are easily accessible, (d) appropriately described and interpreted, and (e) free or almost free. The findings are based on a number of unstructured interviews with potential users, and public consultations with non-governmental organizations, business sector and academia, both of which were conducted in the preparatory phase of the Croatian government’s e-Citizen project [23]. Then established, the Open Government Partnership helped to define the expectations from open data.

A. *All Types of Useful Data*

Users will access the data they need for various purposes. Each users’ community is unique in its own way and has its own needs and priorities in accessing data. We are discussing data consumers’ needs and priorities in Croatia. Although a member state of the EU from July 2013, Croatia is in many aspects a transitional state. The needs and priorities of data consumers in transitional states may be different from the ones in highly democratic EU member states.

The Croatian Parliament recently adopted the new Right to Information Act [15], aligned with the *PSI Directive* [16], and a process of alignment with the *PSI Directive revision* [17] is also planned to be accomplished in next two years. The Open Government Partnership Action Plan for the implementation of the Open Government Partnership initiative in Croatia 2012-2013 [24] has also been created. Consequently, according to the Right to Information Act and other regulation acts, e.g. Public Procurement Act, State Budget Act, etc., a number of datasets has been made available to the public. Open government data web portal is not yet available, although it is being developed [25].

TABLE I. STAKEHOLDERS’ CLASSIFICATION

	Data producers	Data consumers	Data intermediaries	Data specialists
Public sector	Government data producing	Government interoperability		Topic specialization (health, transportation, education, etc.)
Private sector	Business data producing	Data market	Data consultancy	Cross-topic specialization (legal, economic, entrepreneurship, etc.)
Donors, Foundations and International Organizations	Social data producing			
Civil Society Organizations	Mainly social data producing	Data for social good	Data advocacy	
Academia and Research	Science data producing	Data analytics	Data research	Data science
Civic Hackers		Civic data apps development	Apps and visualizations development	
Media		Data journalism		

Although citizens are increasingly aware that greater government transparency and accountability are necessary, government is still not transparent enough. According to the results of online interviews with individuals working in public administration in Croatia, most of them are willing to provide open data to the public.

The state suffers a long recession. The society is encumbered by corruption (Croatia is ranked 62nd according to the Transparency International Corruption Perceptions Index [18]). Opening data to the general public is therefore crucial and of highest priority.

All reasons to make data open apply as we need to achieve (a) transparency and accountability, (b) innovation and economic development; and (c) inclusion, empowerment and law enforcement. Most Croatian citizens list these goals in the same order.

B. *In a Single Place*

Users will prefer to access open data through a single neutral place, i.e., a web portal, where they can find all the available open data. The neutral place, web portal, may be owned by government but it must not mirror any kind of politics, government bodies' relationships, election cycles and other obstacles which will prevent users from trusting open government data.

Who owns and maintains data is a very important question. The owner or steward of open data could be either a web portal or a public (government) agency. Stewardship of open data is particularly important as it manages the quality and timeliness of open data and related metadata.

Following legal requirements, the Croatian Parliament recently set up the position of Information Commissioner [19] whose expected involvement in the implementation of open data will raise confidence, at least in the case of Croatia.

The Croatian Government additionally investigated the treatment of public data by public authorities and was able to prove that it is essential to develop a single open data portal. Since a single public administration portal is being built under the domain gov.hr as a one-stop-shop for all users, it would be logical to have open data published under the same domain, for example, data.gov.hr. This would be in line with similar naming practices for national portals in the EU and the rest of the World (e.g. data.gov.uk, data.gov.it, data.gv.at, data.gov, etc.).

A useful model for using and managing a web portal is shown in Fig. 1 [6]. The model consists of the data user finding data, the data portal acting as single point of access to open data; and the data supplier producing and collecting data. The left-hand side of the Fig. 1 shows the model of direct data provision. The data supplier produces data and collects them (1) at the data portal. The data are published on the data portal (2) and located at the data portal. Users find (3) and obtain (4) data from the data portal. The right-hand side of the Fig. 1 shows the model of indirect data provision. The data supplier produces, collects and publishes data (1). The data are located at the data supplier but the metadata are collected and located at the data portal (2). At the data portal, users find (3) data obtained (4) by the data supplier.

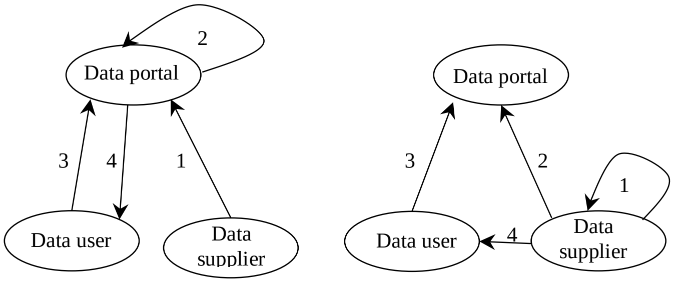


Figure 1. Role of data user, data portal and data supplier

In both models, metadata are located at the data portal making data retrievable through the data portal. In direct data provision model the data are settled at the data portal, and in indirect model at the data supplier. Both models can be implemented on the same data portal, leaving data suppliers to choose between the direct and indirect model of collecting data or metadata.

After starting open data initiative the majority of the open data will be governmental data. There are a lot of data outside governmental sources that may be opened. For instance, business data collected at the chambers of commerce or trade could be opened. In a small community, such as a city, county or even a small country like Croatia, it may be appropriate, at least for budgetary reasons, to have a single place to access all open data.

C. *Easily Accessible and Linkable to Other Data*

In addition to access through a single web portal, the ease of access is of crucial importance. Open data are easily accessible if users can approach all open data through a central metadata portal. It is essential that the metadata portal represents the full repertoire of open data consistently and clearly. A good proposal for metadata repertoire and classification of themes covered by open data is described in [5].

Most of current OGD portals make data available to users of the web portals as downloadable files in formats such as pdf, xls, csv, xml, json etc. Making data available as linked data (LD) through RDF model and RESTful APIs or SPARQL search interfaces is not so common although linked data offers the best practices for publishing and linking data on the web.

To benefit from open data, it is important to allow linking disparate open data sets. The linked open data (LOD) can serve as a platform for new knowledge and can enable new services or applications. Services and application are easier to develop in a LOD environment. Tim Berners-Lee, initiator of linked data, suggests a five stars classification scheme for open data:

- one star: Information is available on the web in any format under an open license
- two stars: Information is available as structured data (e.g. in Excel instead of an image scan of a table)
- three stars: Information is available in non-proprietary formats (e.g. csv instead of Excel)
- four stars: URI identification is used so users can point at individual data

- five stars: Data are linked to other data to provide context. Network effect is achieved.

Achieving full benefit of linked open data can be obtained in the following steps: (a) Analyzing and cleaning data, modeling them by choosing established vocabularies, conversion data to RDF [7], (b) creating an unifier resource identifier (URI) for each data object, (c) choosing appropriate vocabularies for open data or creation of own vocabulary, (d) specification of licenses for re-using data, (e) conversion to RDF. Before publishing, data may be linked to other data, which may increase their value.

The three stars level is considered the minimum for the release of government data for re-use: non-proprietary, machine readable, and accessible via the web. Benefits of linked open data, which are data with four and five stars, include possibilities of linkage to them from any other place, possibilities of bookmarking them and re-using parts of them.

D. *Appropriately Described*

Data should be thoroughly described in order to explain the problem or area to which they relate. The open data description includes metadata described in user's words explaining objects, attributes and relationships between data. The purpose of data initially collected should be explained, i.e., why the data are collected, the context of the data collection, possible applications of data, for what purpose data should not or cannot be used, etc. The data should be declared not to violate privacy principles. Raw data should include full details explaining what the data relates to, how they were collected, who collected them, and how they are formatted.

Data consumer should be aware that re-use of open data should acknowledge the source of data.

E. *Free or Almost Free*

Access to open data should be free. Price of Internet access should be acceptable to all classes of users.

IV. Impediments to Citizens'Adoption of Open Government Data

The impediments to adoption of open government data are many, from political and social to technical. The paper presents a number of impediments to adoption of open government data. The evidence was collected by observing the process of opening the data in Croatia [15], [23], [24], [25] and from discussions with potential open data consumers. Our findings were compared to experiences accompanying open data initiatives in the EU, predominantly in the UK [10]. The majority of impediments noted are quite the same as in communities that have overcome the initial steps in opening data. The presented impediments are listed in the natural order, from those conceptual to technical. Here are, in our opinion, the most significant impediments:

(1) Some citizens do not know or they do not feel that they have the right to seek public information from government and its bodies.

(2) Many citizens are not familiar with the concept and importance of open data. The same findings are seen in advanced communities, such as in the UK where Open data dialogue report [10] finds that participants of the dialogue “found the concept of open data to be abstract and relatively hard to engage with”.

(3) Most citizens cannot precisely differentiate between public and private data.

(4) Many citizens do not feel that seeking public information will make any difference in practical problem solving in their community.

(5) In some, less developed communities, citizens do not have complete confidence in the published public data.

(6) Many citizens do not express an interest in personally exploring datasets. Rather they are more interested in the results and implications of researching open data. The principal benefits of open data are seen to be for researchers rather than the public [10].

(7) Many citizens lack computer knowledge to access open data, and have difficulties in understanding forms and formats of published data.

(8) Many citizens experience the web portal of open government data as not user friendly enough, but only appropriate for computer specialists who are able to work with csv, json, ogd, txt, xls and other formats.

The conceptual impediments (1-5) show that citizens need to become more strongly aware that they have the right to use public data, to enhance their data understanding and their belief in the data. Technical impediments (6-8) show that citizens need to acquire technical skills to access and use the data, or that data should be displayed in a technically acceptable manner.

V. Government Measures for Boosting the Usage of Open Data

To overcome any of previously mentioned impediments and boost the usage of open government data, one or more measures can be implemented. The proposed measures have been derived from experiences accompanying open data initiatives abroad [8], [9], [11], [12] and in Croatia (e.g. e-Citizen project [23], which represents a continuation and the improvement of the public reform process started in Croatia in the last decade; and Open Government Partnership [21], [24], which additionally helps to streamline priorities of opening public processes). The measures are listed in the natural order, as the measures on the conceptual level (1-11) and the measures on the technical level (12-15):

(1) Governments often act as secrecy keepers, not openness leaders. In all countries studied [11], the closed government culture is detected as the barrier to opening data. Government should define a strategy to change its culture by looking at the experiences of leading governments, following various global, regional, citizens' or market initiatives, implementing EU directives or monitoring activities on open data.

(2) Government should provide a useful definition and explanation of both public and open data that is

accepted by law, administration and citizens [8]. A kind of consensus is needed.

(3) In all countries the tensions between open data policy and the privacy of citizens are recognized [11]. Therefore, the difference between open and private data must be clearly defined and explained.

(4) In less developed communities the general public should be educated that it has the right to seek public data. By whom? Self-education, appropriate civil society activities, and clever government initiatives should change the situation. Imposing proper licensing may help [8] in understanding the right to public information.

(5) Marketing of open data is poor. Citizens and interested parties are not sufficiently informed on government’s activities on opening data. The civil society and government itself should do their best to market open data; explain pros of using and re-using open data.

(6) In addition to standard marketing of open data, government should educate citizens to understand and use data [8]. Sharing useful stories and cases of successful open data usage would be helpful. Similar goals have been set in the Open Data Support project [20]. It should open a channel for communicating users’ ideas, proposals for improvement of data or publishing new data, useful successful or unsuccessful cases, impediments etc. through social media or forums. Publisher of open data must be prepared to respond to users’ communication.

(7) Users should be attracted by selecting high value datasets. Datasets may be considered to be of high value if they satisfy the following criteria: data publication is mandatory by law (e.g. regulated by acts, directives, tenders or budget data); the data result from a primary governmental activity (such as health, transportation, financial data); the high level of preparedness of data (already online, such as weather data), or data of high value in general (such as business data). The focus should be on local, specific issues to raise interest for open data, at least at the moment of introducing open data [8].

(8) Non-governmental organizations, charity organizations and business associations have to be involved in open data initiatives [8], [21].

(9) Governments should act like product developers and measure the outcome of their activity. Open data needs to be a product that will improve transparency, accountability, economic, social and other aspects of community.

(10) Government should clearly define and explain to users the difference between public data and private data. Personal data should be confidential, and must not be violated in any way, such as by combination of related datasets. Misunderstanding open data as an attack on privacy prevents full adoption of open data. Government should define and explain to users what open data as opposed to private data are.

(11) In communities where citizens do not have full confidence in the published public information, data openness should be governed through an independent body.

(12) The quality of open data is often questionable or below acceptable limits to permit the publication of data. Even in countries with experience in open data initiatives it is reported [9] that “information is often treated as a black box in the open data movement, information is often seen as a given, used uncritically, and trusted without examination, open data was collected or created for other purposes, it substantial risks for validity, relevance, and trust.” When publishing open data, government has to ensure their quality. Data should be checked for inaccuracies before being opened.

(13) Since many citizens and other users are not keen on personally exploring datasets the web portal should be equipped with as many data applications as realistically possible. A proper user friendly interface would be a catalyst of using open data.

(14) The open data territory in not yet standardized to an acceptable level. The open data portal should use the accepted standards, and reduce number of used formats to the smallest number possible. Its graphical interface should be user friendly. The classification of themes covered by the open data portal should be adjusted to the interests of data consumers and dependent on local circumstances.

(15) The quality of published data may vary from dataset to dataset. New practice of datasets certification such as by Open Data Institute [12] may help “data users to understand its quality, licensing, structure, and its usability, publishers understand how they can better connect with their users, etc.” Certification may be localized, which is better than no certification at all.

VI. Suggested Actions

A general strategy of opening government data should be concentrated on actions in the following areas:

(1) Organizing a single open data web portal (a) supported by adequate technical and organizational infrastructure, (b) by monitoring activities on the portal and constant analysis of data usage in order to be constantly improved,

(2) Stimulating data owners or data suppliers to publish, certify and regularly maintain their data; and

(3) Encouraging end-users to use open data (a) considering users’ feedback using forums or other appropriate tools, and (b) stimulating end-users or data suppliers to develop applications on open data and publish results based on processed data.

All of the actions above represent a challenge. They need to be well planned, performed, monitored, analyzed and continually improved.

VII. Conclusion and Future Work

The key dimensions of implementing open government data as outlined by OECD [14] include challenges related to policy, technology, financing, organization, culture, and legal frameworks. Addressing these challenges is essential in a small transitional community, e.g., Croatia, if we are to create an ecosystem, and build sustainable business models for OGD initiatives that can generate the desired benefits. If not properly tackled, these challenges might obstruct or restrict the capture of benefits of national efforts aimed at spurring OGD.

Additionally, participation of Croatia in the Open Government Partnership has already helped non-governmental organizations, charity organizations and business associations to be involved in open data initiatives.

On the other hand, there are many successful examples of countries which succeeded in opening data. Learning from these examples could streamline Croatia to faster achievement of better results in this area. It has been proposed that additional support be given to the already established collaboration of all interested parties and that already proven technical solutions be reused [22] in order to start with the open data portal in a short period of time.

The paper presented the position and early experience of an open data initiative as seen by end-users in a small transitional country. The future work may consider monitoring the development of the users' perspective on open government data, discuss development and implementation of measures for boosting the usage of open data, analyze the results of their implementation, and compare the results with solutions in other countries or communities.

References

[1] Open Knowledge Foundation, "Open Data Handbook Documentation, release 1.0.0", 2012.

[2] Open Data Institute, "Guides". <http://theodi.org/guides/what-open-data> 6.10.2013

[3] The open definition. <http://opendefinition.org/> 6.10.2013

[4] T.Davies, F. Perini, and J. Alonso,"Researching the emerging impacts of open data," ODDC working paper #1, 2013. <http://www.opendataresearch.org/sites/default/files/posts/Researching%20the%20emerging%20impacts%20of%20open%20data.pdf> 25.10.2013

[5] J. Alonso and C. Iglesias, "Open Data Directory; Use Cases and Requirements," World Wide Web Foundation, 2013. <http://public.webfoundation.org/2013/06/ODD-UCR-Final.pdf> 25.10.2013

[6] E. Kalampokis, E. Tambouris, and K. Tarabanis, "A Classification Scheme for Open Government Data: Towards Linking Decentralised Data," Int. Journal of Web Engineering and Technology, vol. 6, issue 3, June 2011, pp. 266-285.

[7] F. Bauer and M. Kaltenboek, "Linked Open Data: The Essentials," 2012 .<http://www.semantic-web.at/LOD-TheEssentials.pdf> 25.10.2013

[8] M. Fioretti, "Open Data: Emerging trends, issues and best practices," 2011. <http://www.lem.sssup.it/WPLem/odos/odos_report_2.pdf> 27.10.2013

[9] S. Dawes, "A Realistic Look at Open Data," Using Open Data Workshop Brussels, June 19-20, 2012. <http://www.w3.org/2012/06/pmod/pmod2012_submission_38.pdf> 27.10.2013

[10] "Open data dialogue: Final Report," TNS 2012. <http://www.rcuk.ac.uk/documents/documents/TNSBMRBRCUKOpendatareport.pdf> 27.10.2013

[11] N. Huijboom and T. Van den Broek, "Open data: an international comparison of strategies," European Journal of ePractice, Nº 12, March/April 2011. < http://www.epractice.eu/files/European%20Journal%20epractice%20Volume%2012_1.pdf> 27.10.2013

[12] Open Data Institute. Open Data certificate. <https://certificates.theodi.org/> 27.10.2013

[13] G. Vickery, "Review of recent studies on PSI re-use and related market developments," Information Economics Paris, <http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1093> 28.10.2013

[14] B. Ubaldi, "Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives," OECD Working Papers on Public Governance, No. 22, OECD Publishing, 2013. <http://dx.doi.org/10.1787/5k46bj4f03s7-en> 28.10.2013

[15] "Right to Information Act," Official Gazette, No. 25/2013. in Croatian only. <http://narodne-novine.nn.hr/clanci/sluzbeni/2013_02_25_403.html> 28.10.2013

[16] "Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information on the re-use of public sector information," Official Journal of the European Union L 345/9031.12.2003 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:345:0090:0096:EN:PDF> 29.10.2013

[17] "Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information," Official Journal of the European Union L 175/1 27.6.2013 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:175:0001:0008:EN:PDF> 29.10.2013

[18] Transparency International, "Corruption Perceptions Index." <http://cpi.transparency.org/cpi2012/results> 29.10.2013

[19] "Decision on the election of the Information Commissioner," Official Gazette, No. 131/2013. in Croatian only. <http://narodne-novine.nn.hr/clanci/sluzbeni/2013_10_131_2855.htm> 30.10.2013

[20] Open Data Support, DG CONNECT European Commission <https://joinup.ec.europa.eu/community/ods/description> 30.10.2013

[21] Open Government Partnership <http://www.opengovpartnership.org/> 30.10.2013

[22] Data.gov.uk To Go <http://data.gov.uk/blog/datagovuk-to-go> 30.10.2013

[23] "Decision on starting e-Citizen project" Official Gazette, No. 52/2013. in Croatian only. <http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_52_1058.html> 6.1.2014

[24] "Action Plan for the implementation of the Open Government Partnership initiative in Croatia 2012-2013," in Croatian only. <http://www.uzuvrh.hr/userfiles/file/Akcijski%20plan-Partnerstvo%20za%20otvorenu%20vlast-5_4_2012_.pdf> 6.1.2014

[25] "Guidelines for making internet site," Croatian Government, In Croatian only. http://www.vlada.hr/hr/content/download/260703/3840158/version/1/file/Smjernice_za_izradu_internetsjedista.pdf> 8.1.2014

Examining eDemocracy Adoption Intention for Digital Society: An Integrative Model

Omar Al-Hujran
Department of Management Information Systems
Princess Sumaya University for Technology
Amman, Jordan
o.hujran@psut.edu.jo

Mutaz M. Al-Debei
Department of Management Information Systems
The University of Jordan
Amman, Jordan
m.aldebei@ju.edu.jo

Enas Al-Lozi
Department of Management Information Systems
Al-Zaytoonah University of Jordan
Amman, Jordan
Enas.al-lozi@zuj.edu.jo

Abstract— **eDemocracy is one of eGovernment services which aims at fostering public governance and increasing public participation in the governmental decision making process. Our review of related literature revealed that only a paucity of research looked at eDemocracy topic from the adoption perspective, and this is much more evident in the context of developing countries. As such and aiming to fulfill this gap, in this study we aim at examining the adoption intention of eDemocracy in Jordan as a case study from developing countries. To do so, this study develops an integrative model on the basis of Theory of Planned Behavior (TPB) and Technology Acceptance Model (TAM), which are both well-established theories in the field of Information Systems. Results indicate that both perceived usefulness and perceived ease of use are direct predictors of attitude. Further, the results reveal that attitude, subjective norm, and perceived behavioral control directly and positively affect the adoption intention of eDemocracy in Jordan. However, subjective norm was found to have the strongest effect. The study also provides important implications for theory and practice.**

Keywords-eDemocracy; eGovernment; Digital Democracy; Digital Society; Adoption; Theory of Planned Behaviour; Technology Acceptance Model.

I. INTRODUCTION

Electronic government (eGovernment) refers to the use of Information and Communication Technology (ICT) tools and applications so as to enhance transparency and accountability in public administration by improving public service delivery, access to information and services, in addition to governance [26][28][66]. However, the main emphasis of eGovernment is not only on the implementation of new ICT systems per se, but also on how to achieve the strategic goals of governments with the aid of various ICTs. One of the main strategic goals of implementing an eGovernment is the transformation of political systems; the so-called eDemocracy [26][54]. eDemocracy, in the form of greater public participation in decision making process, is expected to move governments forward by enabling effective representative democracy and by enhancing public governance [26]. This study explores the adoption of information and communication technologies and more specifically the internet technology within the context of citizen's participation in democratic processes.

The existing literature on Information Technology (IT) adoption has cover many different contexts, such as IT adoption [8][17][70], eBusiness and eCommerce [36][60][75], eLearning [11][15][56][62], Internet banking [1][24][44][49], mobile services [6][12][73][74], social networking [7][18][53], and eGovernment [5][10][20][22][23][52]. Numerous theoretical models, primarily developed from theories in sociology and psychology, have been applied to evaluate users' adoption new technologies. Among the widely used theories in this domain are the Theory of Reasoned Action (TRA) [4], Theory of Planned Behavior (TPB) [2][3], and Technology Acceptance Model (TAM) [30].

However, the findings of prior research demonstrate that citizen participation in eGovernment remains below expectations in all countries around the world [54]. By examining previous relevant research, one can easily notice that there is only little theoretical grounded studies approaching technology adoption in relation to eDemocracy [57], and more specifically, in developing countries. Hence, aiming to fill this gap, this study integrates TAM with TPB, so as to comprehensively understand the factors affecting the adoption intention of eDemocracy tools in Jordan as a developing country. By doing so, we believe that we could offer some deeper insights to explain the role of technology in citizen's participation.

The rest of this paper is structured as follows. In Section II, the concept of democracy is discussed. In Section III, the related theories (i.e., TPB and TAM) are described. In Section IV, the developed research model and hypotheses are discussed. In Section V, the employed research methodology is described. In Section VI, the study results are presented.

ISBN: 978-1-61208-324-7

Finally, in Section VII, the study results along with their implications are discussed, and conclusions are presented.

II. The Concept of eDemocracy

eDemocracy, sometimes referred to as digital democracy, has received great attention in recent years [43]. There is no universally accepted definition of the eDemocracy concept. Mahrer and Krimmer [54: p.1] define eDemocracy simply as "an approach for increased and better quality citizen participation in the democratic processes". eDemocracy can also be broader and more complex and can be viewed as the use of Internet and its associated technologies (especially Web 2.0 tools) as well as mobile technologies including smart phones to enhance the public governance. It has the potential to provide a new avenue for participation, collaboration, deliberation and engagement in the political process that can make democratic processes more inclusive and transparent [57]. Despite the diversity of eDemocracy definitions found in the literature, there is a common central concept that underlies all these definitions- the assumption of normative goals of eDemocracy: to empower citizen engagement in public consultations for policy making through the utilization of new technologies and to enhance democratic processes and structures [29].

The literature on eGovernment often viewed eDemocracy as a component of overall eGovernment initiatives that aims to allow wider access to, and the delivery of, government information and services [26][54]. In their eGovernment development (i.e., maturity) model, Chatfield and Alhujran [26] proposed eDemocracy as the fourth stage of eGovernment service delivery capability development. This stage of eGovernment service delivery capability enables the public to participate in the process of transforming the government forward towards its democratic goals in terms of improved transparency and governance. Although offering eDemocracy functionalities to the public does not imply that a state or a government will be democratic automatically, greater public engagement is expected to have a positive impact on public governance (i.e., better transparency and accountability) [26].

A considerable amount of literature has already been published on the important role of citizens' participation and engagement towards public-policy making [26][29][67]. Many governments around the globe are engaging their citizens for feedback via their eGovernment websites [67]. By developing eDemocracy capabilities, such as eVoting, online polling mechanism, online surveys, discussion forums and online communities, eGovernment offerings have the ability to exchange opinions and viewpoints on issues that are important to governments and to members of society. eDemocracy including Web 2.0 and social networking sites can be used by governments to empower citizens by enabling them to express their opinions and by offering more opportunities for their voices to be heard by decision makers [67].

Despite the lack of economic resources, Jordan has developed and implemented many successful eDemocracy and eParticipation tools. A recent study conducted by Al-Hujran [9] indicated that the majority of ministries (46 per cent) offer some eDemocracy capabilities to citizens. In addition, the eGovernment program in this country has substantially moved forward in the eParticipation index worldwide, from being ranked 90th in the 2005 United Nations' eGovernment readiness report to 15th in the 2008 report. By using online polling mechanisms, discussion forums and online consultation facilities provided by government websites, Jordanians have the ability to exchange opinions and viewpoints on issues of importance with governments and with other members of society. However, public intention to use the existing eDemocracy tools is remain unexplored. This study is probably one of the first to determine the factors that may influence citizens' adoption of such tools in Jordan.

III. Related Theories: TPB and TAM

Previous research have utilized and employed a number of theories in order to explain users' adoption and acceptance of technologies. This includes Technology Acceptance Model (TAM), Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), Diffusion of Innovation Theory (DOI), Technology-Task Fit (TTF), Unified Theory for Acceptance and Use of Technology (UTAUT), and others. In this study, we aim to integrate two of the most widely adopted theories in explaining acceptance and adoption of technologies, which are TPB and TAM so as to end up with a comprehensive model to examine the adoption intention of eDemocracy technologies by Jordanian Citizens. TPB would help us in examining eDemocracy adoption from a social perspective, whilst TAM is useful to examine the adoption of eDemocracy tools from a technical perspective by highlighting the important roles of usefulness and ease of use. The integration of the aforementioned two models would enable us to get a more cohesive understanding of the phenomenon under investigation from a socio-technical paradigm.

A. *Theory of Planned Behavior*

TPB is considered as one of the most influential theories in predicting and explaining behaviour. Various studies showed the applicability of TPB to various domains, and verified the ability of this theory in providing a valuable framework for explaining and predicting the acceptance of new information technology [47]. According to TPB, people's behaviors are determined by their intentions to perform the behaviour, where their intentions are influenced by attitudes towards behaviour, subjective norms, and their perceived behavioural control. The history of theory of planned behavior is traced back to the theory of reasoned action, developed by Ajzen and Fishbein [4].

The general framework of the theory of planned behaviour postulates three conceptually independent determinants of members' intentions, namely, Attitudes, Subjective Norms, and Perceived Behavioural Control. Attitude towards the behaviour refers to the degree to which a person has a favorable or unfavorable evaluation or appraisal of the behaviour to be acted upon [58][65]. Individual attitude is determined by personal beliefs and traits that characterize that individual in particular. The second determinant strongly relates to social factors and is termed as individuals' subjective norms. Subjective norms refer to the perceived social pressure of the external environment surrounding individuals on whether to perform certain behaviour or not, and how family and friends would affect his/her perception of whether to behave in a certain way or not. This construct is consistently a weaker predictor of physical activity intentions than attitudes and perceived behavioral control [39][40]. The third antecedent of individuals' behavioral intentions is the degree of Perceived Behavioural Control which refers to one‘s perceived ease or difficulty of performing the behaviour [58]. Interestingly, Ajzen [3] assumes that perceived behavioral control reflects to some extent past experience as well as other anticipated hurdles and obstacles (i.e., resources and opportunities available to a person) which might be internal or external.

B. Technology Acceptance Model

TAM focuses on explaining the attitude behind the intention to adopt, accept and use a specific technology or service [63]. It is an adaptation of the TRA from psychology specifically tailored to model user acceptance of Information Technology (IT). TAM has been widely applied in acceptance behaviour across a broad range of IT [10][37][50][51][72]. However, it places more emphasis on the role of technology in affecting users' intentions towards their behaviors.

TAM is primarily built on the TRA, Expectancy Theory [61][71], and Efficacy Theory [19]. It theorizes that one’s behavioral intentions are determined by two specific belief constructs (perceived usefulness, and perceived ease of use). In short, if the central goal is to predict IT adoption from an IT perspective, it can be argued that the TAM is preferable for the reason that it focuses on system design characteristics. TAM predicts whether individuals will accept and voluntary use a certain system.

However, the TAM's fundamental constructs do not fully reflect the specific influences of technological and usage-context factors that may influence users’ acceptance [55]. Therefore, perceived usefulness, and perceived ease of use may not fully explain behavioral intentions towards the use of eDemocracy if not integrated with other social-related factors. Its fundamental constructs do not fully reflect the variety of user task environment and constraints [34]. Moreover, TAM does not take into account the human and social factors that the TPB considers.

IV. RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

Aiming to end up with a model which enjoys a high predictive and explanatory power; we in this study integrate TPB with TAM (see Fig. 1). This is because the Theory of Planned Behaviour takes only social-related factors in explaining and predicting individuals' adoption of technologies, but no technology-related factors are taken into consideration. Moreover, previous studies, for example [65], indicated that TPB's belief structures of intention require a decomposition of attitudinal beliefs if the explanatory power of the theory is to be increased.

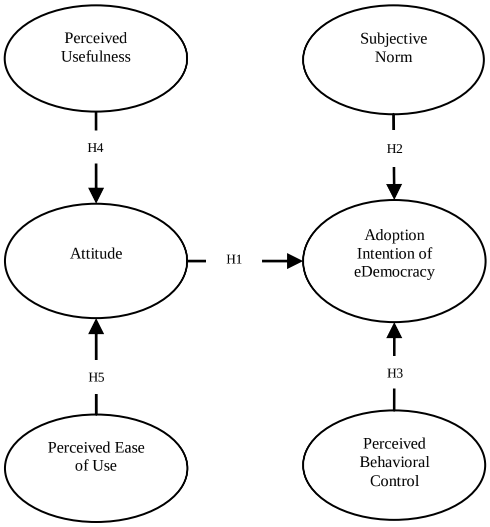


Figure 1. Research Model

Thus, integrating TAM with TPB would overcome the aforementioned limitations given that TAM examines uses' acceptance and adoption of technologies using technology-related factors those reflecting design characteristics. Further, TAM would help in decomposing the attitude construct and thus helps in providing an enhanced explanatory power for the model.

A. Perceived Usefulness

Davis [30: p. 320] defined Perceived Usefulness (PU) as “the degree to which a person believes that using a particular system would enhance his or her job performance”. Previous studies indicated that citizens form positive attitudes toward a technology if they perceive that technology to be useful [5][34][38]. In our case, using eDemocracy tools is believed to be useful as it can be used by governments to enable citizens to express their opinions. This can lead to greater public governance convenience and better transparency and accountability. Thus, this study postulates the following hypothesis.

H1. *Perceived Usefulness directly and positively influences citizen's attitude towards eDemocracy tools.*

B. Perceived Ease of Use

Perceived Ease of Use (PEOU) refers to “the degree to which a person believes that using a particular system would be free of effort” [30: p.320]. In the context of eGovernment, several researchers reported the importance of PEOU as a determinant of the citizen adoption of eGovernment services, either directly or indirectly [5][21][34]. Findings of these studies acknowledged that developing eGovernment websites that are easy to use and more user-friendly would positively influence citizen attitude toward using these services. Based on this discussion, it is believed that citizens are likely to form positive attitudes if they consider their use of eDemocracy tools requires little efforts. Accordingly, we hypothesize the following.

***H2.** Perceived ease of use directly and positively influences citizen's attitude toward eDemocracy tools.*

C. Attitude

Attitude towards the behaviour refers to the degree to which a person has a favorable or unfavorable evaluation or appraisal of the behaviour to be acted upon [3][58][65] and defined by salient beliefs about consequences multiplied by outcome evaluations [46]. Previous studies in studying behavior in the use of technology emphasize the positive relationship between attitude and behavioral intentions [31][69]. In our case, a citizen would evaluate the value of using eDemocracy tools, on the basis of his or her personal beliefs. When citizens believe that the use of eDemocracy as a medium for promoting democratic activities to be positive, they will form strong intentions to use its capabilities. Therefore, this study proposes the following hypothesis.

***H3.** There is a direct positive effect of attitude on the behavioral intention to use eDemocracy tools.*

D. Subjective Norm

The second attitudinal determinant, according to the TPB, strongly relates to social factors and is termed as subjective norm. Subjective norm refers to the perceived social pressure of the external environment surrounding individuals on whether to perform a behaviour, or not [2]. Subjective norm is a function of individual's perceived expectations of important others (e.g., family and friends) and his or her motivation to act in accordance with such expectations. Prior eGovernment, research has investigated subjective norm as a significant predictor of intention to use eGovernment services [34][47]. They found that the subjective norm of citizens positively influences their behavioral intentions. Specifically, in the context of eDemocracy, subjective norm can be recognized as pressure comes from journalists to use recent web technologies such as blogs, wikis, discussion forums, Web 2.0 applications, and other social media to communicate and exchange information promoting democracy. Pressure to use eDemocracy tools may also stem from social referents like peers within the sector, or government. It also may come from eDemocracy rhetoric, discussions, and debates from academics, politicians, practitioners, and the media [57]. In sum, we expect that subjective norm can affect a citizen's behavioral intention to use eDemocarcy tools. Thus, we hypothesize the following.

***H4.** There is a direct positive effect of subjective norm on the behavioral intention to use eDemocracy tools*

E. Perceived Behavioral Control

The construct of perceived behavioral control refers to individual's perception of the amount of control she/he has over carrying out certain behaviour [3]. This perception is closely related to the perception on how easy or difficult to perform the behaviour [58]. Interestingly, Ajzen [3] assumes that perceived behavioral control reflects to some extent situational influences and past experience as well as other anticipated hurdles and obstacles (i.e., resources and opportunities available). Having control over one‘s own behaviour is a major determinant influencing human intentions to participate and engage in a digitally engaged community. In our case, citizen's self-evaluation of his ability to use eDemocracy tools can influence his/her intention to use these technologies. Indeed, eGovernment literature has empirically proven the importance of PBC in determining citizens' intentions to use eGovernment services in general [47] and eDemocracy in particular [57]. Accordingly, a positive influence of PBC on behavioral intentions to use eDemocracy tools is hypothesized in this study.

***H5.** There is a direct positive effect of perceived behavioral control on the behavioral intention to use eDemocracy tools.*

V. Research Methodology

This section is dedicated to show the followed data collection procedure, sample profile, and measurement scales of the model's constructs.

A. Data Collection and Measurement Scales

This is a quantitative study that utilized the survey questionnaire as the main instrument for data collection. Hence, a self-completion, well-structured questionnaire was developed based on previous literature and was then distributed to a random sample and participation was completely voluntary. Prior research showed that the educated Jordanian citizens are the early adopters of the Internet [13] and are likely users of eGovernment and eDemocracy services in Jordan. For this study, therefore, we identify the university students who are Jordanian citizens as our population. A total of 250 questionnaires were distributed to community colleges, undergraduate and postgraduate students in Jordan and 195 questionnaires were returned. Thus, the response rate was (78%). Amongst the 195 returned questionnaires, only six questionnaires were excluded due to multiple skipped questions and missing values. In total, 189 responses (n = 189) were valid and usable for data analysis.

The constructs of interest in this study were “Attitude” (ATT), “Subjective Norm” (SN), “Perceived Behavioural Control” (PBC), and “Behavioural Intention to Use” (BI). The developed questionnaire in this study adapted validated questionnaire items from previous literature with some modifications to fit the specific context of this research. Measurements for subjective norms (SN), attitude (ATT), and perceived behavioral control (PBC) were adopted from [7]. As for behavioral intention to use (BI), perceived usefulness (PU), and perceived ease of use constructs, measurements were adopted from [5] and [59]. All items were measured using a five-point Likert-type scale, ranging from "strongly agree" to "strongly disagree". Table I lists the questionnaire items.

TABLE I. SUMMARY OF MEASUREMENT SCALES

Construct	Item	Measure
Perceived Usefulness (PU)	PU1	Using eDemocracy tools enable me to access relevant information more quickly.
	PU2	Using eDemocracy tools enhances my effectiveness in accessing relevant information.
	PU3	Using eDemocracy tools allows me to access more relevant information than would otherwise possible.
	PU4	Using eDemocracy tools increases my productivity.
Perceived Ease of Use (PEOU)	PEOU1	Learning how to use eDemocracy tools is easy for me.
	PEOU2	I find it easy to use eDemocracy tools.
	PEOU3	My interaction with eDemocracy tools is clear and understandable.
	PEOU4	eDemocracy tools is flexible to interact with.
Behavioral Intention to Use (BI)	BI1	I intend to use eDemocracy tools frequently.
	BI2	I expect that I should use eDemocracy tools in the future.
	BI3	I will strongly recommend others to use eDemocracy tools
Attitude (ATT)	ATT1	I have positive opinion about eDemocracy tools.
	ATT2	I think that the use of eDemocracy tools is good for me
	ATT3	I think that the use of eDemocracy tools is appropriate for me.
Subjective Norms (SN)	SN1	People who influence my behaviour think I should use eDemocracy tools.
	SN2	People who are important to me would think that I should use eDemocracy tools
Perceived Behavioural Control (PBC)	PBC1	How much personal control do you feel have over the use of eDemocracy tools? (very little control/complete control).
	PBC2	How much do you feel that whether your use of eDemocracy tools is beyond your control? (not at all/ very much so).
	PBC3	Whether or not I use eDemocracy tools is entirely up to me

B. Sample Profile

The descriptive statistics of the sample showed that 52.4% of the respondents were male and 47.6% were female. Respondents aged less than 25 years formed the largest age group and represented 72% of the sample, whilst respondents aged between 26-45 years represented 14.8% of the sample. Finally, 13.2% of the respondents aged above 46 years. In terms of their education, the majority respondents (i.e., 74%) are pursuing their undergraduate or community college degrees, whilst those pursing their postgraduate degrees represented only 26% of the sample. The details are shown in Table II.

TABLE II. THE SAMPLE'S PROFILE

Measure	Item	Frequency	Percentage (%)
Gender	Male	99	52.4
	Female	90	47.6
Age	Less than 20	64	33.9
	20-25	72	38.1
	26-45	28	14.8
	46-55	22	11.6
	Above 55	3	1.6
Education	Community college	22	11.6
	Undergraduate	118	62.4
	Postgraduate	49	26

VI. DATA ANALYSIS AND RESULTS

This study utilizes the Structural Equation Modeling (SEM) approach [41], with Partial Least Square (PLS) [42] as an analysis method. PLS has been widely used for theory testing and validation. PLS examines the psychometric properties and provides appropriate evidences on whether relationships might or might not exist [33]. In this study, we performed data analysis in accordance with a two-stage methodology [14] using Smart PLS 2.0 M3. The first step was to test the content, convergent, and discriminant validity of constructs using the measurement model, whilst the second step was to test the structural model and hypotheses.

A. Measurement Model

First, we assessed the reliability and validity of the measurement instrument using content, reliability, and convergent validity criteria. The content validity of our survey instrument was established in two ways. First, the constructs along with their measures which are used in this study were already validated in previous studies as they were all adopted from the existing literature. Second, the results of the pre-test we undertook with subject-matter experts assured content validity of the survey instrument. For reliability of the scale, Cronbach’s alpha, which is a common method used to measure the reliability and internal consistency of scales, was used. Hair et al. [41] suggested that the reliability of the scale is generally accepted if the value of Cronbach’s alpha for each construct is equal or greater than 0.70. The constructs included within the study’s model exhibit a high degree of internal consistency as the values of Cronbach’s alpha ranged from 0.86 (PEOU) to 0.94 (PU), as shown in Table III.

TABLE III. RELIABILITY AND CONVERGENT VALIDITY

Measure	Item	Factor Loading	AVE	CR	Cronbach α
Behavioral Adoption Intention	AI1	0.909	0.868	0.952	0.924
	AI2	0.932			
	AI3	0.953			
Attitude	ATT1	0.901	0.803	0.925	0.878
	ATT2	0.899			
	ATT3	0.889			
Subjective Norm	SN1	0.945	0.892	0.943	0.879
	SN2	0.944			
Perceived Behavioral Control	PBC1	0.880	0.805	0.925	0.879
	PBC2	0.924			
	PBC3	0.886			
Perceived Usefulness	PU1	0.929	0.841	0.955	0.937
	PU2	0.890			
	PU3	0.911			
	PU4	0.937			
Perceived Ease of Use	PEOU1	0.857	0.705	0.905	0.862
	PEOU2	0.776			
	PEOU3	0.855			
	PEOU4	0.868			

A Composite Reliability (CR) and Average Variance Extracted (AVE) tests were conducted to measure convergent validity. Fornell and Larcker [33] suggested that the value of CR for each construct must exceed 0.70 whilst the value of the AVE must exceed 0.50 for the convergent validity to be assured. The CR and AVE values for the constructs included in the study model are all above acceptable levels. Moreover, the standardized path loadings for all indicators were above 0.55 and thus they are all significant [32].

TABLE IV. DESCRIPTIVE ANALYSIS AND DISCRIMINANT VALIDITY

	Mean	SD	AI	ATT	SN	PBC	PU	PEOU
AI	2.77	0.82	**1.00**					
ATT	2.77	0.86	0.48	**1.00**				
SN	2.94	0.78	0.44	0.24	**1.00**			
PBC	2.88	0.69	0.60	0.38	0.23	**1.00**		
PU	2.79	0.97	0.62	0.58	0.35	0.37	**1.00**	
PEOU	2.52	0.68	0.57	0.19	0.33	0.32	0.30	**1.00**

Note: The square roots of the constructs' AVE values are shown in the diagonal line (in bold); non-diagonal elements are latent variable correlations.

As such, content validity, reliability, and convergent validity of the measurement instrument are all satisfactorily met in this research. As for discriminant validity, it is actually established when the square root of the AVE from the construct is greater than the correlation shared between the construct and other constructs in the model [27]. The discriminant validity of the measurement instrument is confirmed in this study given that the square root of the AVE from each construct is larger than all other cross-correlations with other constructs (see Table IV).

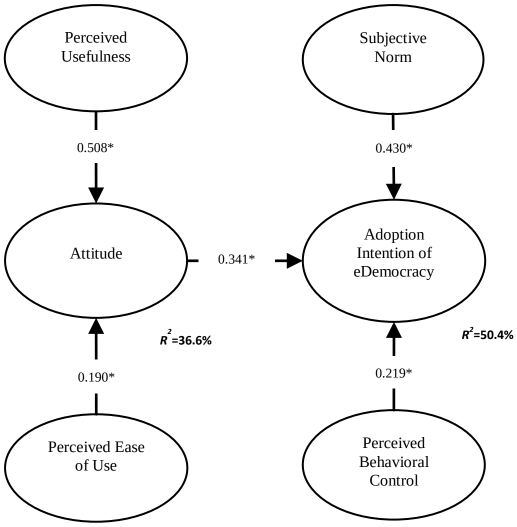
B. *Structural Model*

The results of the PLS-SEM analysis show, as in Fig. 2, the structural model estimation and evaluation of the relationships between attitude, subjective norm, perceived behavioral control and the target construct; i.e., behavioral adoption intention of eDemocracy. Fig. 2 also shows the structural model estimation and evaluation of the relationships between perceived usefulness, perceived ease of use, and the attitude construct. The R^2 value for each endogenous construct (i.e., attitude, and behavioral adoption intention of eDemocracy) was above 25% which demonstrate a highly acceptable prediction level in empirical research [16][35].The coefficient of determination R^2, which is the central criterion for the structural model's assessment [48], has a high value of 0.504 for this study's key target construct; i.e., behavioral adoption intention of eDemoacracy technology. Indeed, the high R2 proves the model's predictive validity [42]. We support the prior finding through the use of Q2 predictive relevancy measure [64]. The obtained Q2 values, after running the blindfolding procedure [27] with an omission distance D=8, were (0.280) for attitude, and (0.404) for the main target construct; i.e., behavioral adoption intention of eDemocracy tools. Both of the Q2 values are well above zero; indicating the predictive relevance of the PLS path model. The bootstrapping procedure was used and we selected 189 cases, 5000 samples, and the no sign changes option to evaluate the significance of the path coefficients [42].

Overall, the results validate the structural model and all hypotheses are supported. Our results indicate that the direct effect of attitude on behavioral adoption intention of eDemocracy has a significant ($p < 0.001$) value of 0.341; the effect of subjective norm on behavioral adoption intention of eDemocracy also has a significant ($p < 0.001$) value of 0.430; and the effect of perceived behavioral control on behavioral adoption intention of eDemocracy also has a significant ($p < 0.001$) value of 0.219. Thus, hypotheses 1, 2, and 3 have been empirically substantiated. Our results also indicate that perceived usefulness and perceived ease of use are two major determinants of attitude ($\beta = 0.51$, $p < 0.001$;$\beta = 0.19$, $p < 0.001$ respectively). Hence, hypotheses 4 and 5 are also supported.

VII. DISCUSSION AND CONCLUSIONS

This study examines behavioral adoption intention of eDemocracy, using an integrative model that integrates two key behavioral adoption models: TPB and TAM. This study contributes to the understanding of inherent predictors of eDemocracy adoption. A major contribution is re-examining salient theories and model and empirically validating a set of interrelationships between key constructs that tend to be associated with behavioral intention by Arabian citizens who have a socio-cultural background different from developed countries in the Europe, U.S., or Asia. It is believed that the research model developed in this study can serve as a foundation for future research on citizen adoption of eDemocracy tools. The overall research findings firmly support the validity of the developed model, accounting for 50.4% of the variances in citizens' intentions to adopt these tools. Specifically, all proposed factors (PU, PEOU, ATT, PBC, and SN) were shown to be significant predictors of citizens' intention to use eDemocracy tools. These findings support the significance of the developed model in predicting citizens' intentions to adopt eDemocracy tools.



*Parameter estimates are significant at 0.001 or less (p < 0.001).

Figure 2. Results of the Structural Model

The results show that citizens' attitude toward eDemocracy is determined jointly by perceived ease of use and perceived usefulness. These findings are consistent with previous TAM research that test and validate the consistent relationships between perceived usefulness, perceived ease of use and attitude [5][25][30][68]. These results suggest that the government should make eDemocracy tools more useful and usable. For example, governments could achieve this by increasing citizens' awareness about the usefulness of using eDemocracy services; providing eGovernment and ICT training workshops; and refining IT/IS systems selections to meet different citizens' needs.

Interestingly, the findings demonstrate that citizens' intention to use eDemocracy tools is importantly influenced by subjective norms. Unsurprisingly, subjective norm was found to have the strongest effect on the adoption of eDemocracy in Jordan. The Arabian culture has a relatively high collectivism orientation [45]. As a result, it is expected that citizens in this region are more sensitive to the social pressures, and have a tendency of accepting their peers' opinions and comply with expectations of important others (e.g., family and friends). This implies that eGovernment officials and policy makers in the Arab countries should carefully manage the peer influence and the social pressure on citizens to assist them to adopt new technologies such as eDemocracy tools.

This study also shows that perceived behavioral control plays a significant role on citizens' intentions to adopt eDemocracy tools. Indeed, such significant role of this construct is evident in the literature [47][57]. This implies that governmental agencies need to provide sufficient resources required to use these tools. It also implies that governments should train and educate citizens to increase their self-efficacy. High self-efficacy users have higher perceived behavior control than other users [47].

As with all studies, this study has its own limitations. This is a cross-sectional study that represents a slice of time and does not show how the citizen's attitude and behavior may change over time. Studies employing a longitudinal design would ascertain whether or not the citizen's attitude toward using eDemocracy tools changes over time, or not. Another limitation is derived from the geographical location of the current research (i.e., Jordan). Although, the findings are believed to be applicable to other Arab countries that share demographic characteristics with Jordan and provide their citizens with the same level of eGovernment in general and eDemocracy in particular, these findings are not necessarily applicable to other Arab countries that lagged behind Jordan in terms of eGovernment and eDemocracy. Therefore, further study in different countries would most likely strengthen and validate the findings of this study.

ACKNOWLEDGMENT

This study is part of a project funded by the Deanship of Academic Research at The University of Jordan, entitled "Determinants of eGovernment Services Adoption and Utilization in Jordan: An Empirical Study".

REFERENCES

[1] E. AbuShanab, J. Pearson, and A. Setterstrom, *Internet banking and customers acceptance in Jordan: the unified model's perspective* Communications of the Association for Information Systems 2010. 26: pp. 493-524.

[2] I. Ajzen, From intentions to actions: A theory of planned behaviour, in Action-control: From cognition to behaviour, J. Kuhl and J. Beckmann, Editors. 1985, Springer: Heidelberg. pp. 1 l-39.

[3] I. Ajzen, The theory of planned behaviour, Journal of Organizational Behaviour and Human Decision Processes, 1991. 50: pp. 179-211.

[4] I. Ajzen and M. Fishbein, Understanding attitudes and predicting social behaviour1980, Englewood Cliffs, NJ: Prentice-Hall.

[5] O. Al Hujran, A. Aloudat, and I. Altarawneh, Factors Influencing Citizen Adoption of E-Government in Developing Countries. International Journal of Technology and Human Interaction, 2013. 9(2): pp. 1-19.

[6] M.M. Al-Debei, A Value-based Approach for Explaining the Adoption Intention of Mobile Data Services. Dirasat: Administrative Sciences, 2013. 40(1): pp. 162-172.

[7] M.M. Al-Debei, E. Al-Lozi, and A. Papazafeiropoulou, Why people keep coming back to Facebook: Explaining and predicting continuance participation from an extended theory of planned behaviour perspective. Decision Support Systems, 2013. 55(1): pp. 43-54.

[8] S. Al-Gahtani, G. Hubona, and J. Wang, Information Technology (IT) in Saudi Arabia: Culture and the Acceptance and Use of IT Information & Management, 2007. 44(8): pp.

681-691.

[9] O. Al-Hujran, An assessment of Jordan's e-government maturity: A user-centric perceptive. Int. J. Electronic Governance 2012. 5(2): pp. 134-150.

[10] O. Al-Hujran, M. Al-dalahmeh, and A. Aloudat, The Role of National Culture on Citizen Adoption of eGovernment Services: An Empirical Study. Electronic Journal of e-Government, 2011. 9(2): pp. 93-106.

[11] O. Al-Hujran, A. Aloudat, H. Al-Hennawi, and H.N. Ismail. Challenges to E-learning Success: The Student Perspective. in International Conference on Information, Business and Education Technology (ICIBIT 2013). 2013. Beijing, China.

[12] O. Al-Hujran and M. Migdadi, Public Acceptance of M-Government Services in Developing Countries: The Case of Jordan, in E-Government Implementation and Practice in Developing Countries, Z. Mahmood, Editor 2013, IGI Global: Pennsylvania.

[13] S. Al-Jaghoub and C. Westrup, Jordan and ICT-led Development: Towards a Competition State? . Information Technology & People, 2003. 16(1): pp. 93-110.

[14] J. Anderson and D. Gerbing, Structural equation modeling in practice: a review and recommended two step approach. Psychological Bulletin, 1988. 103(3): pp. 411–423.

[15] J. Arbaugh, Virtual Classroom Characteristics and Student Satisfaction With Internet-Based MBA Courses. Journal of Management Education 2000. 24(1): pp. 32-54.

[16] S.L. Arlinghaus and D.A. Griffith, Practical Handbook of Spatial Statistics. 1 ed1995, Florida: CRC Press Boca Raton.

[17] E. Baker, S. Al-Gahtani, and G. Hubona, Cultural Impacts on Acceptance and Adoption of Information Technology in a Developing Country Journal of Global Information Management, 2010. 18(3): pp. 35-58.

[18]R.K. Baker and K.M. White, Predicting adolescents' use of social networking sites from an extended theory of planned behaviour perspective Computers in Human Behavior, 2010. 26: pp. 1591–1597.

[19]A. Bandura, Social Learning Theory1977, Englewood Cliffs, NJ: Prentice Hall.

[20] P., Panagiotopoulos, and M.M. Al-Debei. Engaging with citizens online: Understanding the role of ePetitioning in local government democracy. Internet, politics, policy, 2010, pp. 16-17.

[21]L. Carter and F. Bélanger, The utilization of e-government services: Citizen trust, innovation and acceptance factors. Information Systems Journal, 2005. 15(1): pp. 5-25.

[22]L. Carter, L. Shaupp, J. Hobbs, and R. Campbell, The role of security and trust in the adoption of online tax filing. Transforming Government People, Process and Policy, 2012. 5(4): pp. 303-318.

[23]L. Carter, L.C. Shaupp, J. Hobbs, and R. Campbell, The role of security and trust in the adoption of online tax filing. Transforming Government: People, Process and Policy, 2012. 5(4): pp. 303-318.

[24]S. Chan and M. Lu, Understanding Internet Banking Adoption and Use Behavior: A Hong Kong Perspective Journal of Global Information Management, 2004. 12(3): pp. 21-43.

[25] I. Chang, Y. Li, W. Hung, and H. Hwang, An Empirical Study on the Impact of Quality Antecedents on Tax Payers' Acceptance of Internet Tax-Filing Systems. Government Information Quarterly, 2005. 22(3): pp. 389-410.

[26] A.T. Chatfield and O. Alhujran, A cross-country comparative analysis of e-government service delivery among Arab countries. Information Technology for Development, 2009. 15(3): pp. 151-170.

[27] W. Chin, The partial least squares approach to structural equation modeling., in Modern Methods for Business Research, G.A. Marcoulides, Editor 1998, Lawrence Erlbaum Associates: Mahwah, NJ. pp. 295–336.

[28] C. Ciborra and D. Navarra, Good governance, development theory, and aid policy: risks and challenges of e-government in Jordan. Information Technology for Development, 2005. 11(2): pp. 141–159.

[29] S. Coleman and D. Norris. A New Agenda for eDemocracy. 2005 20/10/2013]; Available from: http://ssrn.com/abstract=1325255

[30] F. Davis, Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology. MIS Quarterly, 1989. 13(3): pp. 319-340.

[31] F. Davis, R. Bagozzi, and P. Warshaw, User acceptance of computer technology: A comparison of two theoretical models. Management Science, 1989. 35(8): pp. 982–1005.

[32] R.F. Falk and N.B. Miller, A Primer for Soft Modeling.1992, Akron, OH: The University of Akron Press.

[33] C. Fornell and D.F. Larcker, Evaluating structural equations models with unobservable variables and measurement error. Journal of Marketing Research, 1981. 18(1): pp. 39–50.

[34] J. Fu, C. Farn, and W. Chao, Acceptance of Electronic Tax Filing: A Study of Tax Payer Intentions. Information and Management, 2006. 43(1): pp. 109-126.

[35] A.S. Gaur and S.S. Gaur, Statistical Methods for Practice and Research: A Guide to Data Analysis using SPSS. 1 ed2006, Thousand Oaks, California: Sage Publications.

[36] D. Gefen, K. Elena, and D. Straub, Trust and TAM in Online Shopping: An Integrated Model MIS Quarterly, 2003. 27(1): pp. 51-90.

[37] D. Gefen and D. Straub, Gender Differences in Perception and Adoption of E-Mail: An Extension to the Technology Acceptance Model. MIS Quarterly, 1997. 21(4): pp. 389-400.

[38] D. Gilbert, P. Balestrini, and D. Littleboy, Barriers and benefits in the adoption of e- government. International Journal of Public Sector Management, 2004. 17(4): pp. 286–301.

[39] G. Godin and G. Kok, The theory of planned behaviour: A review of its applications to health-related behaviours American Journal of Health Promotion, 1996. 11: pp. 87–98.

[40] M. Hagger, N. Chatzisarantis, and S. Biddle, The Influence of Autonomous and Controlling Motives on Physical Activity Intentions Within the Theory of Planned Behaviour British Journal of Health Psychology, 2002. 7: pp. 283-297.

[41] J.F. Hair, B. Black, B. Babin, R.E. Anderson, and R.L. Tatham, Multivariate Data Analysis. 6 ed2006, New Jersey: Pearson Prentice Hall.

[42] J.F. Hair, M. Sarstedt, C.M. Ringle, and J.A. Mena., An assessment of the use of partial least squares structural equation modeling in marketing research. Journal of the Academy of Marketing Science, 2012. 40(3): pp. 414-433.

[43] M. Hilbert, The Maturing Concept of e-democracy: From e-Voting and Online Consultations, to Democratic Value Out of Jumbled Online Chatter Journal of Information Technology & Politics, 2009. 6(2): pp. 87-110.

[44] H. Hoehle, E. Scornavacca, and S. Huff, Three decades of research on consumer adoption and utilization of electronic banking channels: A literature analysis. Decision Support Systems, 2012. 54(1): pp. 122-132.

[45] G. Hofstede, Culture's Consequences: International

Differences in Work Related Values,1980, London: Sage.

[46] E. Huang and M. Chuang, Extending the Theory of Planned Behaviour as a Model to Explain Post-Merger Employee Behaviour of IS Use Journal of Computers in Human Behaviour, 2007. 23(1): pp. 240-257.

[47] S. Hung, C. Chang, and T. Yu, Determinants of User Acceptance of the E-government Services: The Case of Online Tax Filing and Payment System Government Information Quarterly, 2006. 23(1): pp. 97-122.

[48] P. Klarner, M. Sarstedt, M. Hoeck, and C.M. Ringle, Disentangling the Effects of Team Competences, Team Adaptability, and Client Communication on the Performance of Management Consulting Teams. Long Range Planning, 2013. 46(3): pp. 258-286.

[49] V. Lai and H. Li, Technology Acceptance Model for Internet Banking: An Invariance Analysis Information and Management, 2005. 42(2): pp. 373-386.

[50] S. Liaw and H. Huang, An investigation of user attitudes toward search engines as an information retrieval tool. Computers in human behaviour, 2003. 19(6): pp. 751-765.

[51] C. Lin and H. Lu, Towards an understanding of the behavioural intention to use a Web site. International journal of information management, 2000. 20: pp. 197-208.

[52] F. Lin, S. Fofanah, and D. Liang, Assessing citizen adoption of e-Government initiatives in Gambia: A validation of the technology acceptance model in information systems success Government Information Quarterly, 2011. 28(2): pp. 271-279.

[53] K.Y. Lin and H.P. Lu, Why people use social networking sites: an empirical study integrating network externalities and motivation theory Computers in Human Behavior, 2011. 27(3): pp. 1152–1161.

[54] H. Mahrer and R. Krimmer, Towards the enhancement of e-democracy: identifying the notion of the 'middleman paradox' Inf. Syst. J., 2005. 15(1): pp. 27-42.

[55] J. Moon and Y. Kim, Extending the TAM for a world-wide-Web context Journal of information and management, 2001. 38(4): pp. 217-230.

[56] H. Motaghian, A. Hassanzadeh, and D.K. Moghadam, Factors affecting university instructors' adoption of web-based learning systems: Case study of Iran Computers & Education, 2013. 61: pp. 158-167.

[57] A. Nchise, An Empirical Analysis of the Theory of Planned Behavior. JeDEM, 2012. 4(2): pp. 171-182.

[58] S. Orbell, S. Hodgkins, and P. Sheeran, Implementation Intentions and the Theory of Planned Behaviour Personality and Social Psychology Bulletin, 1997. 32: pp. 945-954.

[59] P. Pavlou, Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model International Journal of Electronic Commerce, 2003. 7(3): pp. 69-103.

[60] P. Pavlou and M. Fygenson, Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior MIS Quarterly, 2006. 30(1): pp. 115-143.

[61] D. Robey, User attitudes and management information system use Academy of management journal, 1979. 22(3): pp. 73-85.

[62] H.M. Selim, Critical success factors for e-learning acceptance: Confirmatory factor models. Computers & Education 2007. 49(2): pp. 396-413.

[63] Y. Shih and K. Fang, The Use of a Decomposed Theory of Planned Behaviour to Study Internet Banking in Taiwan Journal of Internet Research, 2004. 14(3): pp. 213-223.

[64] M. Stone, Cross-validatory choice and assessment of statistical predictions. Journal of the Royal Statistical Society, 1974. Series B (Methodological): pp. 111-147.

[65] S. Taylo and P. Todd, Assessing IT Usage: The Role of Prior Experience MIS Quarterly, 1995. 19(4): pp. 561–570.

[66] L. Tung and O. Rieck, Adoption of Electronic Government Services Among Business Organizations in Singapore Journal of Strategic Information Systems, 2005. 14(4): pp. 417-440.

[67] UnitedNations. United Nations E-government Survey 2010 2010 [4/10/2013]; Available from: http://unpan1.un.org/intradoc/groups/public/documents/un-dpadmAinpan038853.pdf

[68] V. Venkatesh and F. Davis, A theoretical extension of the technology adoption model: Four longitudinal field studies. Management Science, 2000. 46: pp. 186-204.

[69] V. Venkatesh, M. Morris, G. Davis, and F. Davis, User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 2003. 27(3): pp. 425-478.

[70] V. Venkatesh, J.Y.L. Thong, and X. Xu, Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Quarterly 2012. 36(1): pp. 157-178.

[71] V. Vroom, Work and motivation1964, New York: Wiley.

[72] J. Wu and S. Wang, What drives mobile commerce? An empirical evaluation of the revised technology acceptance model Information and management, 2005. 42: pp. 719-729.

[73] S. Yang, Y. Lu, S. Gupta, Y. Cao, and R. Zhang, Mobile payment services adoption across time: an empirical study of the effects of behavioral beliefs, social influences, and personal traits Computers in Human Behavior, 2012. 28: pp. 129–142.

[74] T. Zarmpou, V. Saprikis, and A. Markos, Modeling users' acceptance of mobile services Electron Commer Res, 2012. 12: pp. 225–248.

[75] Y. Zhang, Y. Fang, K.-K. Wei, E. Ramsey, P. McCole, and H. Chen, Repurchase intention in B2C e-commerce—A relationship quality perspective. Information & Management, 2011. 48(6): pp. 192-200.

Open Source Biomedical Engineering for Sustainability in African Healthcare: Combining Academic Excellence with Innovation

Carmelo De Maria*†‡
Email: carmelo.demaria@centropiaggio.unipi.it

Daniele Mazzei*‡
Email: mazzei@di.unipi.it

Arti Ahluwalia*†
Email: arti.ahluwalia@centropiaggio.unipi.it

*Research Center E. Piaggio, University of Pisa, Largo Lucio Lazzarino 1, 56126, Pisa, Italy
†Department of Ingegneria dell'Informazione, University of Pisa, Via G. Caruso 16, 56126, Pisa, Italy; ‡FabLab Pisa, [1]

Abstract—**Accessible quality healthcare is one of the biggest problems in Africa and other developing countries. This is not only due to the unavailability of resources, but also to the absence of a structured formative process for the design and management of healthcare facilities. Biomedical engineers are known to be the link between technology and medical practice, which is a pillar of healthcare systems in developed countries. In this paper, the Open Source for BioMedical Engineering (OS4BME) project and its kick off summer school are presented. The OS4BME project aims to develop a new generation of biomedical engineers, able to exploit emerging technologies generated by the recent "Makers" revolution. During the one week summer school, students from various sub-Saharan countries have been introduced to these new design, development and sharing paradigms. Students worked together identifying new possible simple biomedical devices, which could help in daily clinical practice. A cheap and easy-to-use neonatal monitoring device was chosen as a Crowd design project. The OS4BME Baby Monitor was designed and assembled by the students during the one week summer school, demonstrating the creative potential of the new generation of biomedical engineers empowered with the paradigms of crowdsourcing and rapid prototyping.**

Keywords-Biomedical Engineering; Open Source; Open Hardware; Crowdsourcing; Africa.

I. INTRODUCTION

While the pillars of healthcare are certainly doctors, clinicians and nurses, at least in the developed world, biomedical engineers are widely recognised as being the cornerstone of any medical facility with high technology diagnostic and therapeutic equipment and devices. The scarcity of accessible quality healthcare in Africa is inextricably linked not only with the lack of resources, but also with the lack of adequately trained biomedical engineers [2]. Excluding South Africa, apart from few singular initiatives (in Nigeria and Ghana), no university in sub-Saharan Africa offers a fully-fledged Biomedical Engineering graduate and post-graduate programme [3]. While several reasons can be identified, certainly the most important is the absence of a clear common understanding of BioMedical Engineering (BME) as a field of study both in higher education as well as in the medical sector. While there are a number of technical level clinical and biomedical engineering courses scattered through sub-Saharan Africa, their quality and content are often questionable [4]. Moreover, medical equipment does not have common standards or operating protocols; indeed in most developed countries, hospitals and clinics have very expensive maintenance contracts with manufacturers who train their own specialized technicians [3]. As a result, the medical device industry in Africa is largely absent and there is an over reliance on foreign companies to repair and design biomedical instrumentation, and resolve technical problems. Very often developed countries donate machines to African hospitals and clinics. While this is an honourable act, the machines usually end up being abandoned when they stop working due to lack of maintenance [5], [6].

The experience of one of the authors in the *ASIALINK* project, "Development of Core Competencies in the areas of Biomedical and Clinical Engineering in the Philippines and Indonesia 2005-2008" [7], [8] has shown us that long term and sustainable improvements can only come through i) recognition on the part of policy makers, of the importance of on loco trained experts capable of managing and repairing biomedical equipment and ii) development of expert skills through individualized programmes that cater to the specific social, cultural and technological needs of a region. These are the two keys to a sustainable and efficient health care system.

However, the world has completely changed with respect to 2006, when the *ASIALINK* project was considered a landmark in South East Asia. The continuous connectivity with tablets, mobile phones, the rapid dissemination of social networks, and the access to free e-learning [9], makes teaching easier and harder at the same time, because of the huge amount of available information.

The world of BME is also changing, here again thanks to various communities that live and discuss on the web. While, a couple of years ago, the development of biomedical devices was essentially linked to companies and universities, now the first examples of open source biomedical devices, such as the Gammasoft Open electrocardiogram and the Smartpulse oximeter are beginning to appear [10], [11]. Although these instruments are not accurate or safe enough to be inserted in the clinical routine, their use can probably save a life more than a damaged, unused (e.g., for high cost) or useless (e.g., because no one knows how to operate) Magnetic Resonance Imaging machine.

Indeed, as The Economist [12] points out in an insightful laymans overview of this burgeoning field, software-reliant devices have also brought on new types of potential risks for patients. The article underlines the difficulty of exposing specific problems with these products, given that medical software (and hardware) is proprietary and patent-protected, thus veiled in secrecy [13]. The open-source approach could, in theory, make it easier to fix, or even avoid, dangerous flaws before they hurt or kill hundreds or thousands of patients. Despite this virtual revolution the mainstream academic community in most countries, developed or not, remains largely ignorant of the potential of open source software, hardware and prototyping. This is particularly evident in Africa - we refer in this paper to sub-Saharan Africa excluding South Africa - where tradition and hierarchy play a strong role at all levels, more so in academia. The authors are of the opinion that academia, and specifically biomedical engineers in higher education, must embrace these new tools, and pass on the message that an Open Source product, developed by a community, without a multinational brand is not equal to un-reliable.

Indeed, today, thanks to crowdthinking and crowdsourcing, the design of several products has an intrinsic revision process, thanks to the community, which has become an active player, and no longer a passive element. The community is the best analyst in terms of quality, reliability and feasibility. While this philosophy is now well accepted in the “software” world, there is still an unjustified unbelief in open “hardware”, because many people are anchored to the consolidated production process, in which product development is affected by high costs due to the inflexibility of fabrication processes (e.g., injection molding). As described in the seminal work of Chris Anderson *“In the next industrial revolution, atoms are the new bits”* [14], [15] 3D printing (later described in the text) is giving everyone, companies, makers, and inventors, the tools that were the exclusive prerogative of a few companies less than ten years ago.

A note of caution however; the freedom given by the Web, and by the possibility to share, fork and re-implement projects, which characterises the Open Source Software, Electronic, and Hardware world, has one major drawback: organizing information (schematics, blueprints) is the boring part that is not always pursued in a passion-driven and self assembled community. In the context of BME however, this latter aspect is critical for ensuring safety and efficacy of biomedical devices, and must go hand in hand with the adoption of open resources for medical applications.

We present here a **position paper** on the benefits and use of Open Source tools and platforms in BME specifically in Africa, which needs to jump on the fastest, cheapest and greenest wagon to growth and self-sufficiency in healthcare. The adoption of these new methods of creating and thinking needs to be coupled with open standards and regulations for medical device safety. We thus argue that the new virtual sharing mentality should be wholeheartedly embraced, valorised and overseen by African universities through a common Open Source for Biomedical Engineering platform (OS4BME) rendering the development, and maintenance of medical equipment accessible to the African continent.

After a discussion on the potential of Crowdthinking (II) and BME in an African context (III), we describe the OS4BME project and its kick-start initiative in Nairobi in 2013 (IV).

II. Crowdsourcing and Crowdthinking Platforms

Currently, there are several resource sharing platforms available on the internet. Their use is spreading throughout the developed World, starting from Europe and the US. The growing accessibility of these platforms, like any shared common resource, has resulted in the generation of huge amounts of garbage. Sifting the useless from the useful is a monumental task and requires experience in design and engineering as well as some skills in negotiating the now cluttered internet of things. More importantly, at present, there are no specific engines or platforms focused on the sharing of biomedical instrumentation and devices. This is because, by their very nature, biomedical devices possess stringent performance requirements to comply with regulatory standards to ensure patient safety.

In the past few years, various studies on social epistemology and group judgment aggregation have been published [16], [17] demonstrating both theoretically and practically the superior heuristic value of collective, non expert, knowledge compared to individual or small group assessment, based on consolidated rules and expectations. In 2006, Jeff Howe coined the Crowdsourcing Neologism in a futuristic article in Wired magazine [18]. Publishing of a neologism related to society cooperation in a magazine instead of in a traditional journal paper is a clear indication of how this new field is driven by a sort of creative talent of the community leading to tangible products for business and non-profit purposes [19].

Crowdthinking platforms are becoming important tools for design and development of new products. Platforms like Wikipedia, Thingiverse, Instructables allow the generation of information that spans from text documents to complex designs and blueprints. Nowadays, various web based communities [20] have an active role in crowd-development and crowd-thinking and also various FabLabs (Fabrication Laboratories) [1] are being born with the aim of bring technology to the people, empowering the creative process with the possibility of building real, physical objects.

In the BME context, we still need a level of supervision, to control the quality and to guarantee the respect of safety standards. By virtue of their access to the brains of the future, universities are the right (and perhaps the only) institutions to properly teach instruments for crowd-“doing”, while giving due importance to concepts, such as ethics, standards and regulations. However, although the latter is at least briefly outlined in university courses, the former sometimes is unknown even to the most brilliant professors.

We define the Crowd, with a capital “C”, as groups of individuals trained and assisted by institutions of technical and higher education, to design, innovate and build together through sharing. As such, the Crowd can and should consist of healthcare providers as well as engineers and technicians. If properly guided by standards and regulations, guaranteed by universities as the organ for control, certification, knowledge and learning, the Crowd is an enabling system for the design and development of medical devices. In addition, the Crowd philosophy can be extended to production processes so fostering local economic growth. In fact, the new methods of production now accessible to all do not require the delocalization of manufacture somewhere else.

III. Contextualization

A. Biomedical Engineering for Africa Today

As Nkuma-Udah et al. point out [3], there are few African universities which offer BME courses. The few that do are based on curricula which were designed for Western universities over 20 years ago and which place undue emphasis on niche subjects like MicroElectroMechanical Systems (MEMs) and cell engineering and less on the learning of new, hard technology and equipment management, maintenance and repair [21]. Evidence from the *ASIALINK* project has demonstrated the value of developing expert skills through individualized programmes that cater to the specific social, cultural and technological needs of a region. While we are not advocating a revolution in BME teaching here, we are strongly in favour of the upgrading of curricula based on solid engineering principles (as outlined by Linsenmeier [22]) with new courses, new technology and new ways of thinking and problem solving, specifically adapted to the needs of countries with few resources. This approach is similar to that proposed by Tzavaras et al. [23] on computer enhanced education laboratories. Fusing the crowd design philosophy with the Biomedical Engineer's objective of improving human healthcare requires that patient safety and efficacy be the paramount concern and also the motivating force behind Crowd driven innovative biomedical device design. Biomedical devices must be designed with safety and efficacy in mind, and they should adhere to regulatory standards (albeit most of the countries in the region of interest have no regulatory authority for biomedical devices). Thus, the Crowd not only needs to be empowered with the technological know-how, but also be given the means to intelligently scan and filter the internet for useful open source materials without being overwhelmed by the choice available. To do so requires fundamental knowledge on biomedical devices, ergonomics, engineering and human physiology: this multidisciplinarity cries out for Crowd. Leaving aside large diagnostic and imaging equipment and prosthetic implants, the vast majority of biomedical devices have a large turnover and no one company monopolizes the market. They are also extremely diverse: examples are plasters, thermometers, hospital beds, sphygomanometers, etc. In this arena, there is huge scope for Crowd driven improvements and innovation.

B. *Social Context*

We are fully aware that although professors, students and technicians maybe very enthusiastic with the idea of open source and Crowd driven biomedical device design, some Ministries of Health, or some powerful economic and other interest groups in developing countries could to be linked to major device manufacturers and therefore can block or hinder our initiative because their interests are threatened. For this reason, part of our project is also focused on creating awareness-raising activities and workshops targeting policymakers, e.g., representatives of the Ministries of Health and Education. Through the help of our funders we will develop advocacy campaigns for the recognition of the importance and relevance of biomedical and clinical engineering in the health care system for creating and managing a sustainable high technology health care system which does not rely on foreign economic aid. Indeed, our aim is to give the universities the tools, guide them through the platform and then let them research the best social conditions (at state level, society level, and so on) to turn the implementation of the project into a success. In fact, we are extremely sensitive about the issue of not imposing our ideas and cultural values on the People of Africa.

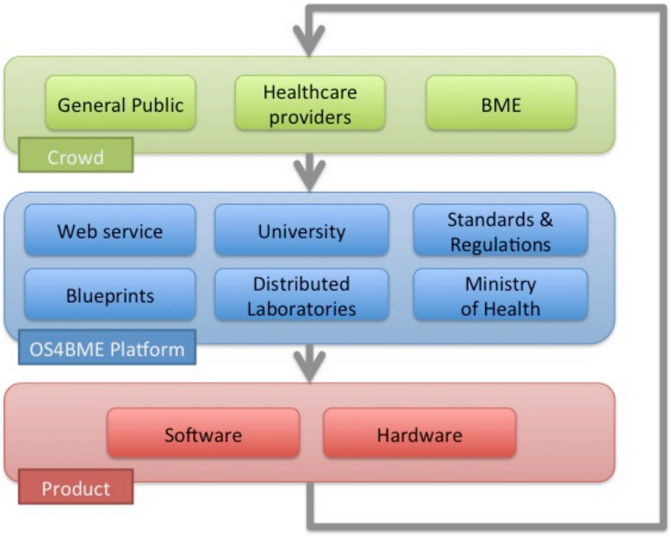


Figure 1. Schematic of the OS4BME work flow.

IV. Teaching the Crowd Philosophy in the BME Context

What we advocate therefore is giving biomedical engineers in sub-Saharan Africa, through their universities, the tools and knowhow in order to design, develop and maintain their own equipment based on the new open hardware and open source revolution, which is happening before our eyes. To achieve this ambitious goal, we outline three main objectives:

- the development of human resources in higher education in Biomedical Engineering in Africa,
- the creation of the OS4BME infrastructure, a sharing, making and repository platform based on the customization and integration of already available web tools,
- the making of a new genre of Biomedical Engineer in Africa equipped with the capacity to exploit and develop innovative designs on the OS4BME platform and of discriminate use of web based and open source resources.

Setting up the OS4BME platform requires the creation of a professional BME working group, versed in the regulatory aspects of biomedical safety and standards, which is able to assess, vet and categorize projects, designs or blueprints and then make them available through the platform open repository. The philosophy is summarised in Figure 1.

A. *Identification of Tools for Crowd Design*

The identification of the most suitable instruments and classroom management and organization is the first step to demonstrate the potential of open source in the BME context. We targeted three main areas of teaching, necessary to give a shape, a brain and to share the ideas:

1) Rapid prototyping: The term Rapid Prototyping (RP) indicates a group of technologies that allows the automatic realization of physical models based on design data using a computer. RP processes belong to the generative (or additive) production processes. In contrast to abrasive (or subtractive) processes, such as lathing, milling, drilling, grinding, eroding, and so forth in which the form is shaped by removing material,

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-324-7

in rapid prototyping the component is formed by joining volume elements. In general, RP techniques follow a Computer Aided Design/Computer Aided Manufacturing (CAD/CAM) approach. The object is designed using a computer (CAD) which then sends the instructions to the machine to obtain the desired shape (CAM), fabricated layer by layer. For the implementation of the RP principle several fundamentally different physical processes are suitable, as photopolymerisation, conglutination of granules or powders by additional binders, extrusion of incipiently or completely melted solid materials [24], [25].

RP was originally conceived as a way to make one-off prototypes, but as the technology spreads more things will printed as finished goods [26].

Although 3D printing is not competitive for mass production (millions of parts), it is perfect in fields where the customization of products is important: because the expense of making tools no longer figures in the equation, the economics of mass production will give way to mass customisation. Parts will then be made in production runs not of a million or even of a few thousand, but of one. Thus, 3D-printed products will continue to creep into the medical, dental and aerospace industries where customers are willing to pay a premium for custom products. In industries that are not built on “markets of one”, 3D printing will help product designers accelerate the design process. 3D printers would also be invaluable in remote areas [27]. Thanks to the various Do-It-Yourself (DIY) communities, several models of Open 3D printers are now available on the Web. One of the most famous is the RepRap community [28] built around the ideas of Adrian Bowyer. He imagined a printer that can print its own parts, and hence through a process of self replication is able to spread this technology throughout the population. All the parts of this type of printer (there are several versions) are open source. The electronics is based on Arduino (see the next section), the software is open source and produces standard G-code files. Designs can be shared and any unprinted parts of the machine are easy to find in any DIY shop. Although, the quality of 3D printed parts made by a RepRap is not high, we believe it is the right starting point to teach the potential of 3D printing to newcomers. The design and printing process is completely transparent so that each step of the complex procedure is easy to follow and replicate.

2) Electronic Prototyping Systems: Until about ten years ago, electronic system design and development was a field accessible only to skilled users, such as engineers, technicians, physicists, etc. Each time an electronic control system was required in a project, the design process had to necessarily include the choice of microcontroller, of a communication system, of a power source, etc. This choice was then binding for the selection of further components, interfaces and programming software. In 2005, in Ivrea (Italy) a team of designers created Arduino [29], a tiny board onto which a microcontroller was mounted together with all the necessary circuits and peripherals required for powering, communication and expansion. A revolution had begun: electronic control systems were not the bottleneck of prototyping anymore. With Arduino, even users without electronics and programming skills could integrate and electronic control system in their own project pushing the limits of complex system design and prototyping. The key factor of the Arduino platform is not only the board but also the easy-to-use programming environment, which allows unskilled users to program through a very intuitive C like programming language. These two factors allowed the birth of a huge user community which empowered the Arduino world through the sharing of code, libraries and projects with open source license. The availability of a pre-made piece of code allowed people to focus their designs on the development of functional and challenging parts using other projects and codes as inputs for their own designs.

The School of Engineering and Technology
Biomedical Engineering Summer School 2013

Figure 2. Group photo from OS4BME class, hosted by the innovator Summer School, in the Kenyatta University conference center.

3) Content Management and Sharing platforms: As highlighted previously, the fast growing DIY community leaves several interesting projects to languish without documentation or with missing parts because a new, more interesting idea was released. Indeed, one of the most challenging aspects of cooperation in design and development is the organization and sharing of information and content. However, thanks to the revolution introduced by the blogging phenomenon, nowadays there are various free and open source Content Management Systems (CMS), which allow an easy and intuitive co-production of documents. These systems have been demonstrated to be useful even for the documentation of engineering and technical projects. MediaWiki [30] in particular is the core engine of the most famous web based encyclopedia Wikipedia. With MediaWiki or similar engines it is possible to create hypertexts made of a huge number of cross-linked pages allowing the creation of very detailed documentations and designs. MediaWiki is designed for the creation of text based documents with embedded pictures and table. Graphics and templates are very minimal allowing users to focus on the real content, which is a core feature of a concurrent design.

B. OS4BME Class

To kick start the initiative and to demonstrate the potential of a regulated open source design and prototyping platform to academics and regulators/decision makers, we proposed a short term intensive course. The course was implemented in August 2013 in Nairobi, Kenya. Our aim was to introduce the OS4BME concept to the African Engineering community and thus create a small working group who will be involved in the set-up of the new platform. To fulfil this objective, the course was focused on the design of a biomedical device from first principles, its assembly and testing and discussion of regulatory issues in device development. The OS4BME course was hosted by the Innovators Summer School held at the Kenyatta University Conference Center, Kenya and took place from the 12th – 16th of August 2013. The Innovators Summer School is an initiative of United Nation Economic Commission for

Africa (UNECA [31]), and is aimed at fostering the economic development of Africa by powering the higher education of the African students. The key player in the initiative is the African Biomedical Engineering Consortium (ABEC [32]), a consortium of African universities with the common mission of bringing excellence to BME in Africa. Over 48 students, technicians and lecturers from the ABEC universities: Kenyatta University (Kenya), University of Nairobi (Kenya), University of Eldoret (Kenya), Addis Ababa University (Ethiopia), Makerere University (Uganda), Kyambogo University (Uganda), Mbarara University (Uganda), University of Malawi (Malawi), Muhimbili University of Health and Allied Sciences (Tanzania), and University of PISA (Italy) attended the course (Figure 2).

After introductory lessons to explain the aim of the course, and some preliminary basics on RP Hardware, software, electronics, and safety regulations; hands-on sessions were provided, giving the students the opportunity to learn by doing. Following the spirit of the course, the free and open CAD/CAM software programs (FreeCAD [33], Slic3r [34], and Pronterface [35]) were adopted to introduce the design approach for 3D printing. For the electronics part, the Arduino platform was selected, for both price, ease of use and flexibility. All documentation was reported using Mediawiki. The keystone of the course was represented by the brainstorming coordinated by the authors with the help of Dr. Molyneux, a pediatrician from the University of Malawi, to understand the problems of a pediatric department in an African hospital context.

The discussion was centred on the respiratory problems of new born premature babies and the monitoring of breathing and body temperature. The aim was to design and build a low cost device, for monitoring respiratory movements and temperature, able to shake the cot to resuscitate the normal breathing of the baby when it stops, and equipped with a sound and light alarm to call a nurse to the cot. The implementation of these features was established together with students, after the brainstorming session. The discussion was focused not only on the functional aspects of the devices, but also on their cost, feasibility safety and reliability, giving the right direction to the project from its start.

After the definition of design specifications, students and attendees were divided into four thematic groups, on the basis of their previously indicated preferences: 1) mechanical design; 2) electronic design; 3) Software design; 4) Standard and regulation identification, and documentation. The subdivision in groups was fundamental in order to keep everyone involved in something they enjoyed: creativity is fed by passion and enthusiasm, boredom kills innovation.

The proposed approach led to the design and fabrication of an open source and low cost baby monitor (Figure 3) in the space of 3 days. The monitor was composed of three modules:

- the elastic band, to monitor the temperature and the breath of the baby;
- a vibrating box, activated when the baby stops breathing for more than 15 seconds;
- a control unit, with a LCD display, 3 LEDs, sound alarms and all the control boards.

Students were encouraged to refer to ISO standards, such as IEC ISO 80601-2-56, with the aim of using these documents to help their work rather than a constraint.

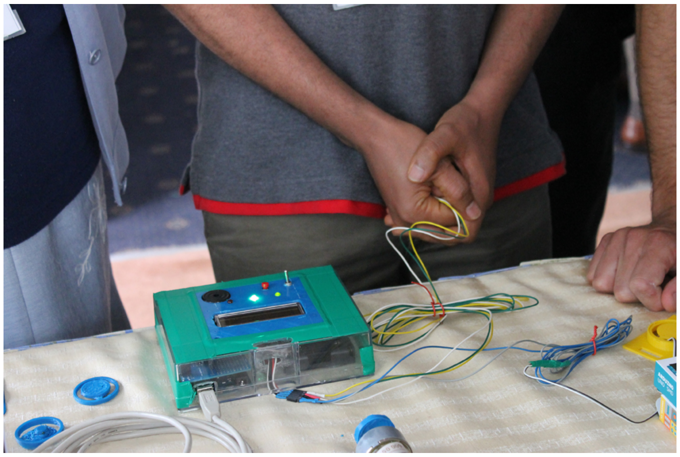


Figure 3. Some moments during the OS4BME class: preliminary test of the device.

At the end of the course an evaluation survey was conducted by the funders. Over 81% of participants expressed extreme satisfaction in the course, although a good proportion (46%) of them could have benefited from more time and previous knowledge on electronics, CAD and programming. In fact, only one participant had previously been exposed to open source technology. There was also interest in the regulatory aspects and standards in medical devices. As the participants were from different backgrounds, many had very little idea what medical devices are and the critical importance of safety issues in such devices. The action thus served to bring home the importance of this aspect during the design of instruments for BME.

V. Conclusion and Future Work

The objective was to develop and nurture resource sharing and technological self-competency through the establishment of a virtual platform containing ideas, blueprints, FAQs and safety regulations for creating new, competitively priced and innovative biomedical devices. We envisage an OS4BME platform managed, regulated and monitored through an academic led pan-African organization, assigned with the task of collecting, classifying, vetting and disseminating information and know-how on the design and development of biomedical devices and instrumentation. In the long term, the sharing of ideas and designs should become the norm, allowing continuous user-driven improvements in healthcare.

A summer school was organized to kick off these ideas, with the aim to create a cohesive working group on which built the platform. The response from students, professors and technicians involved in the school was enthusiastic. It was crucial for participants to play an active role in the identification of the problem, selection of components, design, assembling and testing of the device and in the discussion of regulatory issues in the development of the device. Participants were able to gain a hands-on introduction to electronic system design and programming. All teaching materials, including course documentation, the baby monitor design blueprints are available online for the community to take on and develop further. The 3D printer and all components are now hosted at Kenyatta University's Faculty of Engineering.

Accordingly to the funders' survey the course was an undoubted success. Most students and staff were unaware of the existence of tools, such as Arduino, FreeCad, Slic3r, Media Wiki, etc., let alone the power and implications of open source design and prototyping. The experience was instrumental in bringing this knowledge to the participants, and their keen interest throughout, particularly on 3D printing was apparent.

Although there are several resource sharing platforms available as well as several courses on RP, digital design and embedded electronics, none of these is dedicated to biomedical devices. This is because biomedical devices must be designed first and foremost with patient safety and efficacy in mind. The OS4BME infrastructure, managed by the new genre of biomedical engineers, can be the tool to address this challenge, and its implementation is our objective in the next few years. The first cornerstone of this project was an intensive course, the first of its kind, held in Nairobi addressed safety, ergonomics, biomedical device design, and RP in an integrated manner.

Acknowledgments

The authors would like to thank the UNECA, particularly Dr. Victor Konde for supporting the OS4BME project and financing the summer school. The authors would also like to thank Kenyatta University and in particular Prof. Martin Nzomo and Dr. Daniel Oyoo for the logistic and the local organization of the event. The OS4BME project and the related summer school activities are documented and reported on the ABEC website [32]. Dr. Molyneux was an important source of guidance throughout the summer school. The authors would like to thank also the University of Pisa and the FabLab Pisa for supporting the preparation and organization of the summer school. Part of the electronic material used for the course and for the development of the Baby Monitor was donated by Arduino [29] and the OS4BME experience was reported on their official blog [36]. Finally the authors would like to thank Eng. Giorgio Mattei, Eng. Serena Giusti and Alejandro Callara for their excellent work in supporting and tutoring the OS4BME summer school student groups during the course.

References

[1] [Online]. Available: http://www.fablabpisa.org [retrieved: January, 2014]

[2] S. Mullally, Clinical Engineering Effectiveness in Developing World Hospitals, ser. Canadian theses. Library and Archives Canada = Bibliothèque et Archives Canada, 2008.

[3] K. Nkuma-Udah and E. Mazi, Developing Biomedical Engineering in Africa: A case for Nigeria. Springer Berlin Heidelberg, 2007, vol. 14, pp. 3828–3831.

[4] UNESCO Science Report 2010, Second revised ed. United Nations Educational, Scientific and Cultural Organization, Paris, France, 2010.

[5] A. Jones. Medical equipment donated to developing nations usually ends up on the junk heap. [Online]. Available: http://www.scientificamerican.com/article.cfm?id=medical-equipment-donated-developing-nations-junk-heap [retrieved: January, 2014]

[6] K. H. Courage. Medical technology donations often fail to help. [Online]. Available: http://blogs.scientificamerican.com/observations/2012/08/01/medical-technology-donations-often-fail-to-help/ [retrieved: January, 2014]

[7] A. D. Ahluwalia, "Lessons from asia: Implementing higher education in biomedical engineering for improvement of the healthcare system," in AfricaHI 2012 - The 2nd IASTED African Conference on Health Informatics, Gaborone, Botswana, 2012.

[8] J. Webster, "Strengthening bme in southeast asia [around the world]," Engineering in Medicine and Biology Magazine, IEEE, vol. 26, no. 1, 2007, pp. 10–10.

[9] [Online]. Available: http://www.instructables.com [retrieved: January, 2014]

[10] [Online]. Available: http://www.gammacardiosoft.it/openecg/ [retrieved: January, 2014]

[11] [Online]. Available: http://smartmaker.org/wiki/Projects:smARtPULSE [retrieved: January, 2014]

[12] Open-source medical devices: When code can kill or cure. [Online]. Available: http://www.economist.com/node/21556098 [retrieved: June, 2014]

[13] Z. Bliznakov, G. Mitalas, and N. Pallikarakis, Analysis and Classification of Medical Device Recalls. Springer Berlin Heidelberg, 2007, vol. 14, pp. 3782–3785.

[14] C. Anderson. In the next industrial revolution, atoms are the new bits. [Online]. Available: http://www.wired.com/magazine/2010/01/ff_newrevolution/ [retrieved: January, 2014]

[15] ——, Makers: the new industrial revolution. Random House, 2012.

[16] J. Surowiecki, The wisdom of crowds. Random House Digital, Inc., 2005.

[17] A. Doan, R. Ramakrishnan, and A. Y. Halevy, "Crowdsourcing systems on the world-wide web," Communications of the ACM, vol. 54, no. 4, 2011, pp. 86–96.

[18] J. Howe. The rise of crowdsourcing. [Online]. Available: http://www.wired.com/wired/archive/14.06/crowds.html [retrieved: January, 2014]

[19] G. Fantoni, R. Apreda, D. Gabelloni, and G. Montelisciani, "You solve, i learn: A novel approach to e-learning in collaborative crowdsourcing," in Engineering, Technology and Innovation (ICE), 2012 18th International ICE Conference on. IEEE, 2012, pp. 1–10.

[20] [Online]. Available: http://www.leaninglab.org [retrieved: January, 2014]

[21] T. R. Harris, J. D. Bransford, and S. P. Brophy, "Roles for learning sciences and learning technologies in biomedical engineering education: A review of recent advances," Annual Review of Biomedical Engineering, vol. 4, no. 1, 2002, pp. 29–48.

[22] R. Linsenmeier, "What makes a biomedical engineer?" Engineering in Medicine and Biology Magazine, IEEE, vol. 22, no. 4, 2003, pp. 32–38.

[23] A. Tzavaras, N. Kontodimopoulos, E. Monoyiou, I. Kalatzis, N. Piliouras, I. Trapezanidis, D. Cavouras, and E. Ventouras, "Upgrading undergraduate biomedical engineering laboratory training," in Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the, 2005, pp. 353–356.

[24] A. Gebhardt, Rapid prototyping. Hanser Verlag, 2003.

[25] C. K. Chua, K. F. Leong, and C. C. S. Lim, Rapid prototyping: principles and applications. World Scientific, 2010.

[26] B. Berman, "3-d printing: The new industrial revolution," Business Horizons, vol. 55, no. 2, 2012, pp. 155 – 162.

[27] R. N. Beyers, A. S. Blignaut, and L. Mophuti, "Mobile fablabs: Local and rural innovation in south africa," in Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2012, T. Amiel and B. Wilson, Eds. Denver, Colorado, USA: AACE, June 2012, pp. 112–122.

[28] [Online]. Available: http://www.reprap.org [retrieved: January, 2014]

[29] [Online]. Available: http://www.arduino.cc [retrieved: January, 2014]

[30] [Online]. Available: http://www.mediawiki.org [retrieved: January, 2014]

[31] [Online]. Available: http://www.uneca.org [retrieved: January, 2014]

[32] [Online]. Available: http://www.abecafrica.org [retrieved: January, 2014]

[33] [Online]. Available: http://www.freecad.org [retrieved: January, 2014]

[34] [Online]. Available: http://www.slic3r.org [retrieved: January, 2014]

[35] [Online]. Available: https://github.com/kliment/Printrun [retrieved: January, 2014]

[36] [Online]. Available: http://blog.arduino.cc/2013/10/10/a-baby-monitor-goes-open-source/ [retrieved: January, 2014]

Measuring the Impact of eGovernment Services

Lasse Berntzen
Department of Business and Management
Buskerud and Vestfold University College
Drammen, Norway
e-mail: lasse.berntzen@hbv.no

Abstract – **Impact of eGovernment services is about measurable effects as experienced by stakeholders. Automatic or semi-automatic data collection can make impact assessments more effective, and periodical assessments become more feasible. The paper reviews earlier research on eGovernment impact, discusses the problem of impact as a function of time, and proposes an indicator set suitable for automatic or semi-automatic data collection.**

Keywords – impact; egovernment assessment; indicators; indicator sets; measurements; eGovMon.

I. INTRODUCTION

The Oxford Dictionary of English [1] defines impact as "*a marked effect or influence*".

For e-government services, the definition of impact needs to be refined further. eGovMoNet, an EU-funded thematic network addressing measurement of eGovernment services proposed the following definition [2]: "*The measurable effect of service initiatives that make a difference to its users, providers, or society*". A key concept here is a measurable effect.

The eGovMon project (2008-2012) [3], a research project funded by the Research Council of Norway, worked with municipalities and government agencies to develop methodologies and tools to measure accessibility, transparency, efficiency and impact of eGovernment services.

According to the eGovMon project proposal, impact was described as "*a measurable positive effect of a service on a web site, e.g. number of visitors, user surveys explaining level of satisfaction with the service*."

Another definition by Millard and Shanin [4] links impacts to general objectives of eGovernment: "*These are the overall goals of a policy and are expressed in terms of its ultimate impacts. These will not normally be expressed as eGovernment objectives, but rather as societal objectives to which successful eGovernment development should contribute, such as economic growth, jobs, democracy, inclusion, quality of life, etc.*"

Measuring impact is not easy for two reasons:

- Impact is multi-dimensional and potentially very complex. An easy way out is to focus on a very limited set of indicators, but simultaneously running the risk of loosing key aspects that makes a difference to the stakeholders (citizens/users, service providers, society).
- Impact is also a function of time. A measurement will never be more than a snapshot of something happening over time.

Note that impact can be positive or negative, based on what kind of difference it makes to its stakeholders. If the impact is positive or negative needs to be addressed from the perspective of the respective stakeholder.

This paper aims at providing a short overview of research on impact of e-government, discuss some of the complexities involved, and finally, propose how impact data can be collected and used for automated or semi-automated measurements.

II. RELATED WORK

There has been limited research on the measurement of eGovernment impact. Except from a few academic papers from around 2004-2005 (described below), most recent search results refer to eGovMoNet thematic network and the eGovMon project (described above).

In one of the first papers discussing impact in the context of e-government [5], Peters, Janssen and van Engers observed: "*Our analyzes shows a messy picture on the measurement of e-government. Many measurement instruments take a too simplistic view and focus on measuring what is easy to measure. Many of the instruments focus on measuring the visible front of eGovernment and ignore the performance of the cross-agency business processes. None of the instruments focus on measuring multi-service organizations. The instruments focus on one (type of) agency and do not provide an overall picture.* " Their conclusion was: "*A good theoretical framework for measuring the impact of eGovernment and the use of resources is still lacking*".

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-324-7

Aichholzer [6] analyzed the impacts of e-Government in Austria. He based his analysis on case studies and found the following impacts:

- Reduced process time
- Improved service
- Reduced administrative burden
- Increased efficiency
- Adaption problems and reorganization
- Cost reductions and enhanced revenues

He stated that his analysis was "*still largely in its infancy*", and that "*comprehensive and methodologically sound assessment frameworks for measuring e-government effects are not yet at hand*".

Amberg et al. [7] used a stakeholder approach to find different impacts of eGovernment. The stakeholder analysis revealed the following stakeholder groups, and relevant impacts for each group:

Citizens (individual and collective)

- Improved information (quantity and quality)
- Increased quality of service offerings
- Increased citizen- friendliness and comfort of application flows and services
- Availability of online service offerings 24 hours a day
- Time savings (*)
- Financial savings (*)
- Increased (perceived) transparency of application flow
- Improved communication with rural and remote communities
- Increased involvement and participation in decision processes at communal level (e-democracy)

Private sector and non-profit organizations

- Improved information (quantity and quality)
- Time savings (*)
- Financial savings (*)
- Increased information and service delivery transparency
- Increased quality of service offerings
- Improved communication possibilities for organizations in rural and remote communities

Employees

- Increased motivation
- Job enrichment and new forms of functions
- Personnel development (*)
- Reduced work load
- Improved working conditions

Internal organization

- Reduced costs (*)
- Increased revenues (*)
- Increased process efficiency (*)
- Modernization of IT/communication infrastructure (capacity) (*)
- Improved organizational image as a result of better location marketing
- Increased financial aids and donations (*)

Central government politics

- Improved intercommunal communication and collaboration
- Reduced costs (*)
- Improved efficiency (*)
- Improved location marketing and image
- Acceleration of decision processes in public administration (*)

The authors proposed methods to evaluate each effect, for most of them qualitative surveys and personal interviews and for some (*) measurements of operating figures. Such data would typically be accessible from other computer-based systems (e.g. ERP-system) through a protocol or an interface.

The authors ended up with a proposal for a scoring template (Figure 1) for "measuring the total impact of e-government".

The scoring template uses a scale from 0 (insignificant) to 10 (significant) to evaluate the effects on each single stakeholder. Each single effect is assigned a weight. Each stakeholder group is also assigned a weight. The score for each effect is multiplied with the weight and the weighted scores are added together to give the total impact score.

	Evaluation	Weight each effect	Weight stakeholders
Effects on:	(0-10) (E)	(W)	(E x W)
Citizens			**40%**
effect C1	--x--------	20%	8%
effect C2	-------x---	80%	32%
Private sector			**20%**
effect P1	-----x-----	50%	10%
effect P2	---x-------	50%	10%
Employees			**15%**
effect E1	----x------	80%	12%
effect E2	--------x--	20%	3%
Organization			**15%**
effect O1	---x-------	60%	9%
effect O2	x----------	40%	6%
Central government			**10%**
effect G1	----------x	50%	5%
effect G2	-----x-----	50%	5%

Figure 1. Template for measuring total impact of eGovernment [7]

In parallel with these efforts, other researchers have found easier ways to assess e-government [8]:

- Counting the number of eGovernment services or making a checklist of "most important" eGovernment services.

- Measuring the maturity of e-services based on their complexity or level of integration.
- Measuring the accessibility or usability aspects of eGovernment services.

The common approach is to address the supply-side. What electronic services do the government provide? How many and how good are the services?

Only a small ratio of papers and reports address eGovernment services from the citizen or user perspective (e.g., Norris [9]). What is the uptake of a service? How satisfied are the users?

Impact is about mixing both perspectives (supply side and demand side) with even more dimensions, e.g. uptake and satisfaction, to understand the total effect of eGovernment services.

The problem is to find indicators that are relevant and preferably possible to collect through automated procedures.

Heeks [10] investigated the measurement of impact. He found the following samples of measure: citizen benefit, financial benefit, back-office changes. Samples of indicators were; time saved, financial savings perceived by officials, nature of changes to government processes, and changes in process time. The data gathering methods used were: interview, internal self-assessment, questionnaire, popup survey.

He ended up with the following recommendation:

> "**Output/Impact Measurement**
> *Measures beyond adoption in the eGovernment value chain are needed to judge the value of eGovernment. Most of the impact examples given in Table 3 (of Heek`s paper) were measured by self assessment; a method with distinct drawbacks, as noted below. As also discussed later, there may be emerging opportunities to use web metrics/crawlers to assess some outputs/impacts but only in certain situations. In general, then, output and impact measurements require some form of survey. Surveys have been used for this but survey data to date seems to have concentrated mainly on adoption and use, so there is obvious potential for change.*"

Millard and Shahin [4] also links impacts and general objectives: "*Outcomes are converted to impacts (defined as the general objectives) by the ICT-enabled policy achievement intervention logic. Impacts are at the societal level, and encompass what eGovernment outcomes should contribute to. This could include*:

- *economic productivity*
- *economic growth*
- *jobs*
- *competitiveness*
- *local and regional development*
- *environmental improvement and sustainable development*
- *inclusion*
- *democracy, participation and citizenship*
- *quality of life / happiness*
- *increased justice and security*
- *universal human rights and peace*

The consulting companies Deloitte Consulting and Indigo [11], working on behalf of the European Commission, published a study on the measurement of eGovernment user satisfaction and impact.

The introduction says:

> "*The European Commission Information Society and Media study on measurement of user satisfaction and impact has developed a multilayer user-satisfaction and impact measurement toolkit aimed at providing both policy makers and public agencies with the necessary information and tools for the analysis of public sector service provision. This standardized survey framework provides a hands-on approach to a set of customizable survey tools*".

But, when discussing measurement of user impact, the report focuses on effectiveness, giving the following examples:

- reduced administrative burden – examples: % change in time and costs saved by citizens and businesses, or in number of users reporting e-service saved time over traditional methods for a standard bundle of services;
- increased users' value and satisfaction – examples: % change in waiting times for a standard bundle of services, or in number of users reporting eGovernment services to be useful;
- more inclusive public services – examples: % increase of eGovernment use by socially disadvantaged groups, or of number of SMEs bidding for public tenders electronically.

This short literature review shows the complexity as well as the almost endless possibilities that exist for making indicators.

III. A MODEL TO UNDERSTAND IMPACT

Stragier, Verdegen, and Verleye developed the model shown in Figure 2, to describe the relationship between input, output, outcome and impact [2,12]. The eGovMoNet thematic network used this model.

The model shows the following four types of outcomes from eGovernment: benefits, barriers, uptake and satisfaction, which again makes impact on different stakeholders/stakeholder groups.

By collecting information on benefits (e.g. improved efficiency, transparency and/or quality), barriers (e.g., accessibility barriers), uptake (ratio or number of users) and satisfaction (through e.g., user satisfaction surveys), it would be possible to compute an impact score for each stakeholder/stakeholder group.

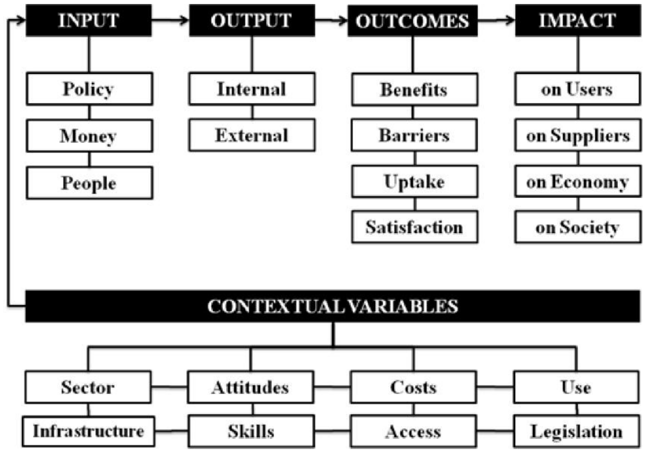


Figure 2. Framework for measuring impact [2,12].

IV. One problem: Impact and time

Impact can have several dimensions and be seen as a function of time. Therefore a measurement can show one dominant type of impact at time t1 and another type of impact at time t2. Ideally, impact is measured relative to time t0, before the service is made available.

One illustrative example: A municipality introduces an eGovernment service to handle application for kindergartens. The use of this service is mandatory. Parents experiencing problems are advised to visit the municipal service center for help and instruction. Most parents experience no problems with the service, but a few feel they lack the necessary competence to use the service. The employees working at the service center get some complaining visitors ("everything was better before"), but spend time showing them how to use the system.

The short-term impact is that most users adopted the electronic service, but the introduction also created a high level of noise. The administrative gains for the administration were not very high.

However, the following year, due to efforts put in the first year, things went more smoothly, with almost no complaints and increased efficiency.

This shows that impact is something fluid that changes over time. It is only possible to take snapshots of impact.

V. How to measure impact

For the eGovMon project it was necessary to balance an almost unlimited number of possible dimensions of impact with the need for an effective data collection regime. Therefore, eGovMon did not address long term impact of eGovernment services, but more the short-term effects as seen by citizens/users and administration. It was also necessary to select indicators that could be collected automatically or with limited effort.

The indicators were developed and discussed during workshops with eGovMon partners (municipalities and public agencies).

Two stakeholder groups were identified:

- Citizens/users
- Administration

For the first stakeholder group, the following outcomes were identified:

- Benefits
- Barriers
- Uptake
- Satisfaction

For the second stakeholder group, one outcome was identified:

- Benefits

Even if it would be possible to identify barriers, uptake and satisfaction from the administration side, these outcomes are less relevant since eGovMon targets existing services. Therefore, potential barriers have already been removed; the uptake is in place (the administration processes the results of the service), and at this stage, should the administration not be satisfied with the service, it is their own problem.

This gives the following set of five indicators:

- Benefits for the citizen/user
- Barriers experienced by the citizen/user
- Uptake by citizens/users
- The satisfaction reported by the citizen/user
- Benefits for the administration

A. Benefits for the citizen/user

One of the benefits addressed already is the efficiency gain for the user. Other benefits may be faster response, access from everywhere at any time, and better quality. As a starting point, the efficiency gain for citizens/users is selected as indicator, with the possibility to incorporate other aspects at future times.

B. Barriers experienced by the citizen/user

Barriers include access to technology, accessibility and appropriate training. Since access to technology is not seen as a problem in Norway (the digital divide is almost non-existent), the accessibility score can be used as an indicator. Since services often are provided through forms, it may also be beneficial to address certain specific issues e.g.

- Prefilled content
- Validation of fields where appropriate
- Help information available
- Meaningful error messages (in user's own language)

- For multi-page forms – possibility to move back and forth
- Possibility to provide user feedback (feedback button)
- The possibility to complete a form after a break (no timeout)

C. *Uptake by citizens/users*

Uptake would typically be the ratio between users of the electronic service and the total number of (potential) users.

D. *The satisfaction reported by the citizen/user*

Satisfaction can be reported through electronic surveys, or even better, a small survey upon exit. “Please rate your overall satisfaction with this electronic service”.

E. *Benefits for the administration*

The efficiency gain for the administration has been addressed earlier. Other benefits may include quality improvement of data submitted due to built in validation of forms.

The scores of each of the five indicators can be normalized (e.g., on a scale from 0 to 20) and then be added to produce an impact score (e.g., 0 to 100).

VI. Conclusion and Discussion

In this paper, we have given an overview of some previous attempts to measure eGovernment impact, and also proposed a new set of indicators. Following Heeks [8], self-assessments have been avoided, and focus has been put on data collection by web metrics/crawlers and surveys. Data collection can then be made automatic or semi-automatic. The proposed indicator set tries to balance ease of use with the complexity of impact analysis. The indicator set uses five indicators to measure impact both from the citizen/user side and from the administrative side, and can be used for longitudinal studies of impact.

Acknowledgment

The eGovMon project was co-funded by the Research Council of Norway under the VERDIKT program. Project no.: VERDIKT 183392/S10.

The author wants to thank the eGovMon core team for valuable input and discussions.

References

[1] Oxford English Dictionary, Oxford University Press, 2006

[2] Verleye, G., Karamagioli, E., Verdegem, P., Jenner, S. and Lorenzo, E. Measure Paper 3; Impact measurement. https://www.academia.edu/1020911/Measure_paper_3_Impact_measurement [Retrieved Feb 2014]

[3] eGovMon Project Folder http://archive.tingtun.no/eGovMon/folder_egovmon_org.pdf [Retrieved Feb 2014]

[4] Millard, J., Leitner, C. and Shahin, J. Towards the eGovernment vision for EU in 2010: research policy challenges. Institute for Prospective Technological Studies. 2006. http://ftp.jrc.es/EURdoc/eur22635en.pdf

[5] Peters, Rob M., Janssen, Marijn and van Engers, Tom M. Measuring eGovernment Impact: Existing practices and shortcomings. Proceedings of the 6th international conference on Electronic Commerce, ACM, New York, 2004, pp. 480-489.

[6] Aichholzer, G., Service Take-Up and Impacts of E-Government in Austria. In Wimmer, M. et al. (eds.). Electronic Government, Proceedings 4th International Conference EGOV 2005. Lecture Notes in Computer Science 3591, Springer. 2005, pp. 93-104.

[7] Amberg, M., R. I. Markov, et al. A Framework for Valuing the Economic Profitability of e-Government. Proceedings of the 1st International Conference on e-Government ICEG 2005, Academic Conferences, 2005, pp. 45-55.

[8] Berntzen, L, & Olsen, M.G., "Benchmarking e-Government - A Comparative Review of Three International Benchmarking Studies," Proceedings, Third International Conference on Digital Society (ICDS), 2009 pp.77-82

[9] Norris, D. F. e-Government Impacts at the American Grassroots: An Initial Assessment. Electronic Government. Proceedings of the 3rd Internatinal Conference EGOV 2004, Lecture Notes in Computer Science 3183, Springer, 2004, pp. 371-376.

[10] Heeks, R. Understanding and measuring eGovernment: International benchmarking studies, United Nations http://unpan1.un.org/intradoc/groups/public/documents/un/unpan023686.pdf, 2006 [Retrieved Feb 2014]

[11] Deloitte Consulting and Indigov (2008) Study on the Measurement of eGovernment User Satisfaction and Impact. European Commission http://www.epractice.eu/files/EU%20UserSat_Final%20Report.pdf [Retrieved Feb 2014]

[12] Stragier, J., Verdegen, P., and Verleye, G. (2010) “How is e-Government Progressing? A Data Driven Approach to e-Government Monitoring”, Journal of Universal Computer Science, vol. 16, no. 8, 2010, pp. 1075-1088.

Business Models Analysis for Multiplex Operators in the Process of Digitization

Kemal Huseinovic
Radio and Monitoring
Communications Regulatory Agency
Sarajevo, Bosnia and Herzegovina
khuseinovic@rak.ba

Meliha Dulic
Radio and Monitoring
Communications Regulatory Agency
Sarajevo, Bosnia and Herzegovina
mdulic@rak.ba

Jasmin Musovic
Radio and Monitoring
Communications Regulatory Agency
Sarajevo, Bosnia and Herzegovina
jmusovic@rak.ba

***Abstract*—This article examines two business models for multiplex (MUX) operators in the process of digitization: Business model 1, where a MUX operator rents the existing network infrastructure and Business model 2, where a MUX operator owns the network infrastructure. By examining these models, this article aims to show which business model and which standard are most cost efficient for digital television implementation in Bosnia and Herzegovina. This analysis shows that a good MUX operator business model is very important for digital television implementation. Three different scenarios point to the fact that the transmission system significantly affects the cost of the MUX operator. Through this analysis, it will be determined that Business model 2 is more economical for Bosnia and Herzegovina.**

Keywords-broadcasters; business models; investment costs; legal framework; MUX operator.

I. INTRODUCTION

Regional Radio-communication Conference RRC-06 was held in Geneva, from 15 May to 16 June 2006 with a goal of setting the plan of spectrum usage for the radio diffusion needs in Europe, Africa and parts of Asia. According to GE-06 agreement, the process of transition to digital broadcasting is to be done in Very High Frequency (VHF) III (174-230 MHz) and Ultra High Frequency (UHF) IV/V (470-862 MHz) bands. This agreement states June 17, 2015 as the date of completion of the transition process [1].

Digital television allows broadcasters to offer new and different services to its customers, which include significantly improved reception, with fewer interruptions and errors in transmission, wide screen format, Standard Definition Television (SDTV), High Definition Television (HDTV), high quality sound, Electronic Program Guide (EPG), radio programs, multicasting and data casting [2].

The provision of digital television requires MUX operator that provides television and radio programs, digital content added services, electronic communication services and other associated identification signals and data.

Since digital broadcasting has still not begun in Bosnia and Herzegovina, this paper provides a brief overview of the situation in Bosnia and Herzegovina. After that, potential business models will be proposed for MUX operators. In accordance with the analysis of the situation in Bosnia and Herzegovina, economic analysis will be carried out in order to determine which digital television standard is best for implementation, and thus determine which business model is the optimal one.

II. DIGITAL TELEVISION IN BOSNIA AND HERZEGOVINA

A. Regulatory and Legal Aspects od Digital Terrestrial Television Introduction

Bosnia and Herzegovina initiated the process of transition to digital broadcasting in time. By establishing the Digital Terrestrial Television (DTT) forum of Bosnia and Herzegovina (in 2006), with operational work of the secretariat and working groups (in 2007), and based on a debate in the communications sector and successful regional cooperation in this field, the Council of Ministers has adopted the strategy document for the transition to digital broadcasting in 2009. This strategy document provides guidance to the relevant institutions in this area, informs interested parties in the communications sector and approaches this subject to citizens. As the development and adoption of the action plan, proposed in a strategy document, are in a serious delay, the steps required for analogue broadcasting turn off could not have been implemented until December 1st, 2011, as was scheduled by the strategy [3].

B. Technological Aspects of DTT Introduction

The key players for DTT introduction are shown in Figure 1, adapted from [4]. This figure shows that there are three key players in the process of delivering digital services:

1. Content and Application Service Providers (CASP) provide content and applications and after that this content is distributed towards interconnection points with Network Service Providers (NSP), where such content is concentrated and packed with contents from other CASPs.
2. NSP provides program transmission to DTT MUX operator where the content is selected from the transmission network, and via DTT multiplexes forwarded to the transmitting site. One NSP is able

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-324-7

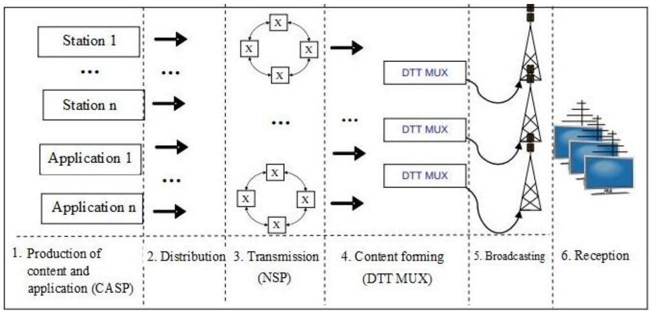


Figure 1. Key players in DTT market.

to transmit a greater variety of TV programs in its own network, while DTT MUX operator selects only those TV programs that have a license to broadcast in the network of that DTT MUX operator.

3. DTT MUX operator collects and marks the content and sends it as a digital multiplex, and then decides which Conditional Access (CA) and which Subscriber Management System (SMS) will be used.

Using the three key players has the following benefits [5]:

- Fast network disconnection, which is achieved by the NSP setting the transmitter, while the MUX operator is oriented to the SMS system, multiplexing and distribution;
- Increasing expansion of services;
- Smaller investments, because they are distributed to all three key players.

Disadvantages of having three key players are [5]:

- Higher complexity of the process of delivering content to users;
- As all three sides are mutually dependent on each other in the process of delivering the content to users in a case that one party violates the regulatory requirements, it causes inconvenience to other parties, as well as the disruption of service provision.

In order to avoid these shortcomings, there could be only two key players, CASP and MUX operator [5]. This way, complexity of the process of digital services delivery to end users is reduced and the management of the entire process is much easier. In this approach, MUX operator assumes the role of providing the infrastructure and management of the entire transmission process.

III. BUSINESS MODELS FOR MUX OPERATORS

Business modeling, and analysis of technical and economic aspects of business strategies and opportunities, has an increasingly important role in scientific research. Various researchers, in different contexts, presented several different definitions of business models. Teece [7] talk about importance of business models:

"Whenever a business is established, it either explicitly or implicitly employs a particular business model that describes the architecture of the value creation, delivery, and capture mechanisms employed by the business enterprise. The essence of a business model is that it defines the manner by which the business enterprise delivers value to customers, entices customers to pay for value, and converts those payments to profit: it thus reflects management's hypothesis about what customers want, how they want it, and how an enterprise can organize to best meet those needs, get paid for doing so, and make a profit."

Each MUX operator should be supported by a successful business model. A MUX operator is essentially a service provider as a standardized signal flow for digital broadcasting systems. That flow, in addition to television and radio programs, includes additional digital services, electronic communications services and other associated identification signals and data.

The main MUX operator functions can be summarized as follows:

- Establishing, operating and developing multiplexes;
- Providing and managing connections with the CASPs;
- Providing and managing the delivery of multimedia services to end users;
- Compliance with the requirements of regulators, in accordance with the permit.

The number of MUX operators in one country depends on how much coverage should be achieved or for which broadcasters MUX operator is intended.

Regarding the coverage, we have the following MUX operators [5]:

- MUX operators for national coverage;
- MUX operators for regional coverage;
- MUX operators for local coverage.

Regarding their purpose, we have following MUX operators [5]:

- MUX operators for public broadcasters;
- MUX operators for commercial broadcasters;
- MUX operators for value added services.

For the digital television broadcasting, in the beginning, it is recommended to use two MUX operators, one MUX for public broadcasters (MUX A) and one MUX for commercial broadcasters (MUX B, by allotments), where a public MUX can also broadcast commercial CASP services in order to encourage the competition [5]. The existence of one MUX operator for value added services in the begginig of this process would be counter productive and would not make any sense from a business aspect.

Two potential business MUX operator models will be described in the next section. Participants, their relationships, streams of revenue and cost generators are presented for each model.

The black arrows in each of the business models represent the direction of the flow of services, while revenue streams are represented by red arrows. The ellipse on each scheme represents a participant, while a rectangle inside the ellipse represents the role of the participant. One participant may have one or more roles.

TABLE I. INCOME AND OUTCOME FLOWS FOR KEY PLAYERS

Players	Roles	Income		Outcome	
		Interface	Flow	Interface	Flow
MUX operator	Content aggregation and multiplexing, network provider	Cont_Whl	Subscription for content transmission	Cap_Whl	The cost of content transmission
		VA_Ser	Subscription for value added services transmission	Internally	Attracting customers, marketing, commissions, charges, aggregation, multiplexing and transmission costs, operations, upgrade, and maintenance costs for DVB access and transmission networks
Content provider	Content provider	Subscription	Subscription for the content and advertising	Cont_Whl	The cost of purchasing the rights of content owners and subscription fees for the transfer of content
Content producer	Content producer /content owner	Cont_Whl	Revenue from the sale of rights to content provider	Internally	Investment cost for creating new content
Value added services provider	Value added services provider	Subscription	Revenues from end users for value added services	VA_Ser	Subscription fees for the transfer of content
				Internally	Investment cost for creating new services

A. *Business Model 1 – Digital Broadcasting in which MUX Operator Takes a Lease of the Existing Network Infrastructure*

The business model that is shown in Figure 2 describes the scenario of providing broadcasting services to the end user. MUX operators obtain the content in the wholesale from various participants and also have a role of content collectors, by collecting more TV programs or data sequences on the broadcast channel. On the other side, NSP manages the broadcasting network and sells the capacity to MUX operator. In other words, MUX operator does not own the network infrastructure, so it rents it from NSP. It is important to mention that, in case of commercial content providers, their income does not come from subscriptions for content usage, as is the case with public content providers, but from the companies that advertise through them. The key participants in this model are MUX operator, NSP operator, content provider, content producer, the owner of content, and value added services provider.

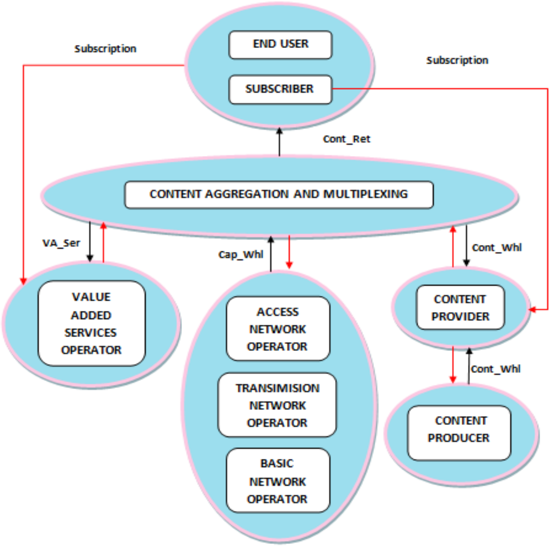


Figure 2. Business model 1 – Digital broadcasting in which MUX operator rents the existing network infrastructure.

Table I shows flows of income and outcome for key players in Business model 1.

B. *Business Model 2 – Digital Broadcasting in Which MUX Operator Owns Network Infrastructure*

Business model 2 is shown in Figure 3.

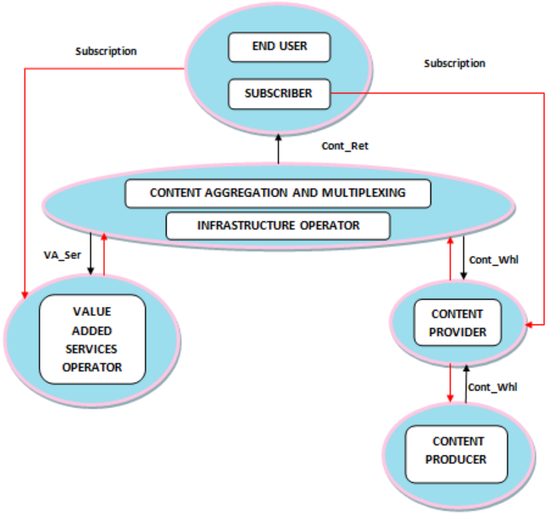


Figure 3. Business model 2 – Digital broadcasting in which MUX operator owns network infrastructure.

TABLE II. INCOME AND OUTCOME FLOWS FOR KEY PLAYERS

Players	Roles	Income		Outcome	
		Interface	Flow	Interface	Flow
MUX operator	Content aggregation and multiplexing, network provider	Cont_Whl	Subscription for content transmission	Cap_Whl	The cost of content transmission
		VA_Ser	Subscription for value added services transmission	Internally	Attracting customers, marketing, commissions, charges, aggregation, multiplexing and transmission costs, operations, upgrade, and maintenance costs for DVB access and transmission networks
Content provider	Content provider	Subscription	Subscription for the content and advertising	Cont_Whl	The cost of purchasing the rights of content owners and subscription fees for the transfer of content
Content producer	Content producer /content owner	Cont_Whl	Revenue from the sale of rights to content	Internally	Investment cost for creating new content
Value added services provider	Value added services provider	Subscription	Revenues from end users value added services	VA_Ser	Subscription fees for the transfer of content
				Internally	Investment cost for creating new services

IV. ECONOMIC ANALYSIS OF INTRODUCING MUX OPERATORS IN BOSNIA AND HERZEGOVINA

This section provides a cost estimation for the construction of MUX network for commercial broadcasters, MUX B. This study is based on the fact that the coverage of population with digital signal is proportional to the current coverage with analog signal. UHF channels are assigned to MUX B and it can transmit up to 8 programs on one channel. This means that the MUX operator revenues will be by 8 emitters. During the construction of this network, there is one MUX operator with national coverage. In the business world, the optimum time for paying back the invested resources is 8 years, so this analysis will also take 8 years as the time for paying back investments for MUX operators. In addition to that, this analysis has predicted the period of nine months as the optimal time to install the necessary equipment.

Initial costs are all those costs that MUX operator will have prior to equipment installation and start-up. These costs include purchase of head-end system equipment, transmission system and transmitter system. Also, these costs may include the cost of paying for permits and purchase of frequencies [6].

Both initial and total costs of MUX operators depend on which transmission system will be used, as well as the price that CASPs will pay to MUX operators. All initial costs are shown in Table III.

In order to determine which transmission system is the most economical, three scenarios will be considered to estimate the total cost of MUX operator.

TABLE III. INITIAL COSTS OF MUX OPERATOR

Initial costs parameter	Price(EUR)
Head-end system	250,000.00
Work permit (first year)	15,000.00
Satellite segment renting (first year)	2,000,000.00
Transmission links renting (first year)	1,000,000.00
Satellite transmission system equipment	383,000.00
Terrestrial transmission system equipment	2,000,000.00
Transmitter system equipment	8,000,000.00

A. Scenario 1 – Total Costs of MUX Operator in a Case When a Transmission is Done via Satellite

As the transmission is done by using a satellite, it is necessary to rent a satellite segment. According to Table III, we have following investment costs:

- Head-end system – 250,000.00 EUR*;*
- Work permit – 15,000.00 EUR;
- Satellite segment renting – 2,000,000.00 EUR;
- Satellite transmission system equipment – 383,000.00 EUR;
- Transmitter system equipment – 8,000,000.00 EUR.

The total initial costs amount to 10,648,000.000 EUR. After these costs, it is necessary to install the purchased equipment. In addition, payment of work licenses, frequency renting and satellite segment renting contribute to the amount of total costs. Also, a significant part of the costs come from the electronic equipment amortization, where the rate of amortization is 20%. All of the costs mentioned above are shown in Table IV.

The total costs for this scenario are approximately 34,230,000.00 EUR. At the annual level, these costs amount to 4,300,000.00 EUR. If we take into consideration that

MUX operator serves 8 emitters, the annual fee for one emitter in this scenario is approximately 540,000.00 EUR.

B. Scenario 2 – Total Costs of MUX Operator in a Case When a Transmission is Done via Rented Terrestrial Links

In this case, a MUX operator rents links for transmitting content towards transmission sites. Initial costs are now:

- Head-end system – 250,000.00 EUR*;*
- Work permit – 15,000.00 EUR;
- Transmission link renting – 1,000,000.00 EUR;
- Transmitter system equipment – 8,000,000.00 EUR.

All costs that the MUX operator has in this scenario are shown in Table V.

The total costs for this scenario are approximately 25,500,000.00 EUR. At the annual level, these costs amount to 3,187,500.00 EUR. The annual fee for one emitter in this scenario is approximately 400,000.00 EUR.

C. Scenario 3 – Total Costs of MUX Operator in a Case When the Operator Owns the Transmission Network

In this scenario, a MUX operator owns a transmission network. This means that it needs to buy transmission system equipment and install it. Therefore, the initial costs will change. According to this, we have the following investment costs:

- Head-end system – 250,000.00 EUR*;*
- Work permit – 15,000.00 EUR;
- Transmission system equipment – 2,000,000.00 EUR.
- Transmitter system equipment – 8,000,000.00 EUR.

All costs for MUX operator, for this scenario, are shown in Table VI.

The total costs for this scenario are approximately 21,300,000.00 EUR. At the annual level, these costs amount to 2,660,000.00 EUR, which means that annual fee for one emitter in this scenario is approximately 350,000.00 EUR.

TABLE IV. SUMMARY OF MUX OPERATOR COSTS FOR SCENARIO 1

Cost parameter	Price (EUR)
Total initial costs	10,648,000.000
Costs of satellite transmission system equipment installation	39,000.00
Costs of transmitter system equipment installation	2,355,000.00
Work permit costs	105,000.00
Costs of frequency renting	100,000.00
Costs of satellite segment renting	14,000,000.00
Costs of satellite transmission system equipment amortization	325,000.00
Costs of transmitter system equipment amortization	6,658,000.00

TABLE V. SUMMARY OF MUX OPERATOR COSTS FOR SCENARIO 2

Cost parameter	Price (EUR)
Total initial costs	9,265,000.00
Costs of transmission links renting	7,000,000.00
Costs of transmitter system equipment installation	2,355,000.00
Work permit costs	105,000.00
Costs of frequency renting	100,000.00
Costs of transmitter system equipment amortization	6,658,000.00

VI. SUMMARY OF MUX OPERATOR COSTS FOR SCENARIO 3

Cost parameter	Price (EUR)
Total initial costs	10,265,000.00
Costs of transmission system equipment installation	55,000.00
Costs of transmitter system equipment installation	2,355,000.00
Work permit costs	105,000.00
Costs of frequency renting	100,000.00
Costs of terrestrial transmission system equipment amortization	1,665,000.00
Costs of transmitter system equipment amortization	6,658,000.00

D. Result Analyzis

The cost recovery Curves of the MUX operator for the three analyzed scenarios is shown in Figure 4.

Initial investment costs are highest for Scenario 1, which is primarily due to the payment of satellite segment rent at the beginning of the year. The minimum initial investment costs are for Scenario 2, because the costs of renting transmission links at the beginning of the year are less than half in comparison with renting a satellite segment.

The costs increase significantly in an eight year working period. A large contribution to those costs is renting a satellite band for Scenario 1, or renting transmission links for Scenario 2. These costs do not exist in the third scenario because the MUX operator has its own network.

The graph shows that the fastest payment refund is in the third scenario, where the curve has the highest slope. In one moment costs for the third scenario become lower than the costs in the second scenario. The reason for this is that in Scenario 3 MUX operator has its own network, so there is no need to pay for equipment renting.

Concerning the MUX operator, we can conclude that for digital television transmission in Bosnia it is best to use terrestrial transmission with its own transmission network, because the total cost is smaller, as well as the price that broadcasters would have to pay. It means that for MUX operator is better to use Business model 2. Because of the lower costs, broadcasters would be more inclined to agree to digitize their signals and transfer the same.

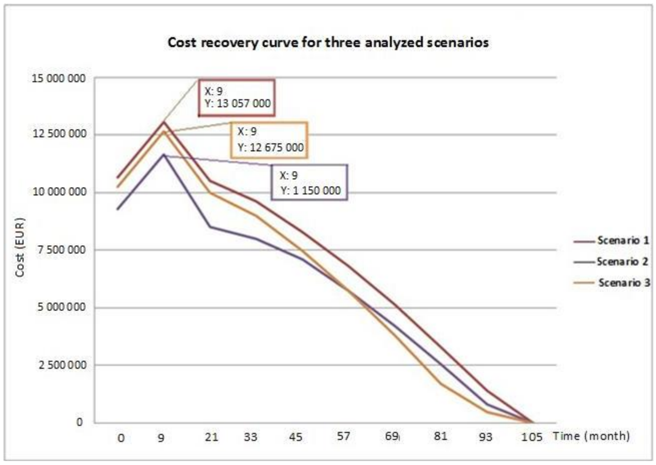


Figure 4. MUX operator cost recovery curve for three analyzed scenarios.

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-324-7

The advantage broadcasters get in this case is the availability of their programs throughout the country.

By entering into this business, one can accurately calculate the costs that are expected for MUX operators and the price broadcasters will have to pay. Based on that price, it is possible to win over broadcasters before starting the operations, so the risk of investing in this business is low.

V. Conclusion and Future Work

Transition to digital broadcasting frees the RF spectrum of the digital dividend, which has very favorable characteristics and provides an optimal balance between transmission capacity and coverage range.

The use of MPEG-4 standard for video compression and the use of DVB-T2 transmission technology, with a goal of more efficient use of the frequency spectrum, by facilitating the transmission of a higher number of channels per frequency, is an interesting option, especially for countries that have not yet completed the process of transition to digital broadcasting.

Two previously mentioned business models can be used as a startup framework for the implementation of MUX operator. The cost of introducing a MUX operator depends on the transmission system as could be seen from the economic analysis. The lowest costs that are expected for MUX operators are in the case of terrestrial transmission where MUX operator owns the network. In this case, the price paid by broadcasters is much lower and it is a great advantage, because that way the broadcasters will be more inclined to enter the process of digitization.

If there was a jump-start with a DVB-T2 standard in Bosnia, it would mean higher investment costs, approximately 100,000.00 EUR. In this case, the number of programs on one channel would increase to 16. This further leads to a much larger contributions. In that case, the MUX operator can reduce the cost of transmitting content to broadcasters and thus attract more broadcasters and increase the competition and interest in the market.

MUX operator would also transmit value added services such as interactive services, internet, etc. So their revenues would probably increase.

References

[1] Communication Regulatory Agency, „Economic analysis of the need to introduce new services in Bosnia and Herzegovina“, Sarajevo, December 2012.

[2] Web: DigiTAG – Digital Terrestrial Television Action Group, www.digitag.org [retrieved: January, 2014].

[3] Communication Regulatory Agency, "Analysis of the legal framework for the introduction of DTT in [Bosnia and Herzegovina" project, Version A-1.1, 2012.

[4] DTT Forum of Bosnia and Herzegovina, “The strategy of transition from analogue to digital terrestrial broadcasting in the bands 174-230 MHz and 470-862 MHz in Bosnia and Herzegovina”, 2009.

[5] Rwanda Utilities Regulatory Agency, „Managing the change from analogue to terrestrial digital broadcast in Rwanda“, January 2008.

[6] Tanzania Communication Regulatory Authority, „Public consultation document on establishment of cost based transmission fee for digtial terrestrial television (DTT) charged by multiplex operators to content service providers“, November 2012.

[7] D. J. Teece, Business Modelfs, Business Strategy and Innovation, Long Range Planning 43, 2010, pp. 172–194.

Towards an Interoperability Evaluation Process for Mobile Contactless City Service

Serge Chaumette, Damien Dubernet, Jonathan Ouoba
LaBRI, University of Bordeaux
Bordeaux, France
{serge.chaumette, damien.dubernet, jonathan.ouoba}@labri.fr

Erkki Siira, Tuomo Tuikka
VTT Technical Research Centre of Finland
Oulu, Finland
{erkki.siira, tuomo.tuikka}@vtt.fi

Abstract— **Interoperability of mobile contactless city services has been emerging as a topic of discussion in many of the recent events by the representatives of industry and city organizations. Evidently, the interoperability has a connotation of a world where systems and devices interoperate or work together seamlessly. In the real world, such interoperability is a myth, and must always be built by considering the specificities of the existing artefacts. This paper studies and defines interoperability in the context of mobile contactless city services. We present three piloted mobile contactless city services to identify which kind of interoperability issues can be raised. Based on this analysis, an interoperability framework is proposed first by delineating the set of relevant entities and then by presenting four dimensions of the interoperability issues between the entities. We believe that this framework helps finding other related elements to make a coherent picture of interoperability in this context. It also leads to the definition of a relevant evaluation process. The goal of the paper is: (1) to properly define interoperability in our context; (2) to propose a set of evaluation criteria; (3) to propose an overview of an evaluation process**

Keywords-interoperability; seamless; cities; contactless; NFC; mobile services; user

I. INTRODUCTION

Mobile phones have become a commodity and are increasingly in use by urban dwellers. One of the emerging technologies for the mobile services is contactless technology, already known in city or smart cards. This can be considered to be the next paradigm change in the smart city end-user services. When the mobile contactless technology becomes more common, also other smart city services will appear, combining payment, loyalty, and city services.

Mobile contactless services in smart cities are and will be based on Near Field Communication (NFC). NFC means, simply put, an upgrade to usability of a mobile device; the user can touch a reader with the mobile in a similar manner as with a contactless card [13].

The work presented in this paper is carried within the Smart Urban Spaces Project abbreviated as SUS (www.smarturbanspaces.org). One of the objectives of the SUS project was to reach a certain level of interoperability regarding mobile contactless city services deployments and interactions. Then, it was necessary to define a framework. The role of the framework is to help understand the environment of mobile contactless city services, to analyze the relations between the different stakeholders (in legacy systems and services to be deployed) and also to provide relevant information concerning the level of interoperability that can be reached. For an end-user, interoperability simply means that the services and systems work together so that a service can be accomplished. Looking simply at technological interoperability does not help sufficiently when mapping the service opportunities or analyzing the smart city services. Technological level, which consists of hardware and software, will not guarantee service level usability or the service success. Taking into account all these factors deserve a more general approach and a clear view of the environment where the services exist. Then, in our attempt to unfold the term interoperability through a framework dedicated to mobile contactless city services, it was essential to enlarge the focus on aspects such as usability, business cases, regulations, etc.

The questions that have guided our work and that lie at the core of this paper are as follows: what are the elements to consider when building such a framework to analyze the interoperability in the context of contactless city services? What should be the form of the evaluation process, related to the interoperability framework, which needs to be implemented? The work presented in this paper details the main basis and the first practical elements regarding the development of a complete evaluation process.

In the following section, we give elements related to the mobile services context. We more precisely expose the mobile contactless city services concept and we shortly explain how the NFC technology that enables it operates. Section 2 also provides a definition of interoperability, presents in more details the interoperability issues raised by the specificities of the SUS project and propose an approach to address these problems. Section 3 mainly deals with the interoperability framework proposal and section 4 describes the resulting evaluation process. Eventually, section 5 presents the next steps to follow in the complete achievement of the evaluation process.

II. CONTEXT

A. Mobile Contactless City Services

City services around the world are different and they are dependent of the local culture, laws, etc. Transform a city service into a mobile city service requires a certain amount of technological advancement and maturity that is not the same for each city service. For example, SMS-based information and ticketing services have been around over 10 years already. As technology has gone forward, the NFC technology has become a promising enabling technology for various city services. From the user perspective it is a new mean of interaction with the environment that is based on the touching paradigm [14]. Mobile phone is essential in a sense that it is the central mean for the user to connect to the content information or make an action such as payment [6]. NFC, which is a wireless communication technology derived from Radio Frequency Identification (RFID), has three kinds of modes: the reading and writing tags mode, the peer-to-peer mode which enables connections between two mobile phones, and the card emulation mode. These modes are all enablers for new city services, e.g., for tagging the city [8], access control [7], home care with sensors [12] or city tourism [2].

Initiatives, which are mainly research demonstrations and pilots, have shown the interest in contactless services for the benefit of citizens in cities. The SmartTouch project, that brought together European industrial and academic partners, has particularly proved the added value of NFC in ticketing and transportation by contributing to the deployment of real services on the field [11]. Another notable example is the Cityzi project [3] allowing users to access in French cities of Nice and Strasbourg, a bunch of contactless services (in the field of transport, event management, car parking and banking) by using their NFC-enabled mobile phone.

B. Interoperability Overview

Interoperability is usually defined as Wegner does in [15] as “the ability of two or more software components to cooperate despite the differences in language, interface, and execution platform”. Consequently, the most usual approach to interoperability is to consider it simply as a technological issue. For instance, securely managing smartcard applications in NFC devices [9], considerations on how to develop applications on top of an operating system [4], the ecosystem perspective [10], or multi-application approach as done by [1] are some examples. This approach generally leads to propose a service assessment model [5] based on 5 levels: the signature level, the protocol level, the semantic level, the quality level, and the context level.

Aforementioned view seems too restrictive in our context because it only takes into consideration the technical aspects. Of course, interoperability of mobile contactless city services is an issue that comes up in discussions especially on tourist scenarios when a tourist would need to use a local bus or to buy a train ticket. However, the interoperability concept is a larger issue in the mobile contactless city service context, though. In addition to interoperability of technology, such as software architecture, protocol level or looking at how devices and services communicate between each other, a ubiquitous and contextual contactless mobile service deserves a deeper consideration on the emerging services themselves. As far as we know, there is a lack of appropriate models to study the role of the essential players interacting in the context of the deployment and the use of contactless services for smart cities. Our conception of interoperability goes beyond the traditional approach, in that it is necessary to provide background information and analysis taking into consideration the whole ecosystem (at the legal and business level for example) that represents a city or even a network of cities.

C. Examples of Issues in Interoperability in the Context of SUS Project

There were 49 piloted and planned services in the SUS project. From there we can see the challenges in the interoperability of a mobile contactless city service concept. The difficulty lies in the fact that it is necessary to take into account all aspects of interoperability that could affect the deployment of such services and analyze the interactions between the different players involved in the development and the exploitation. To highlight some of the interoperability issues that may arise, we give examples of SUS city services: Daycare, Small Event Ticketing and Open Europeans 2011. The Daycare service provides a solution for registering children to the day-care by using passive NFC tags and mobile phones. The Small Event Ticketing service proposes a system to manage ticketing operations (issuance and validation) for small events with NFC-enabled mobile phones. Regarding the Open Europeans 2011, it provided a control access system (with smart cards and mobile phones) for the sailing competition held in Helsinki.

Technical interoperability issues were not uniform. One service was encountering standardization failures within NFC ecosystem (the Small Event Ticketing service that uses the NFC peer-to-peer mode) while the other was encountering the difficultness to integrate legacy backend systems refitted to be mobile and contactless (Daycare). Usability and social interoperability issues were also raised and demonstrated the need to motivate and educate the users. For example, the Daycare case needed 1200 employees to be trained and the motivation to use the system was in the reduction of routine paperwork that allows the employees to spend more time in the real work with the children. A learning curve for users has been observed in all of the services. From the business side of interoperability, the presented services had different kind of parties involved. For the sailing competition case, the local transportation authority smart cards were used during the piloting phase. Thus, the sailing competition access control case was dependent of the business decisions of another company.

D. An Approach to Analyze the Interoperability

We have been involved with close to ten workshops on how to delineate the smart city services in European cities together with services providers, city representatives, application developers, and infrastructure developers. During the effort we delineated and presented a set of entities in the use case ecosystem: Mobile, User, Service, Infrastructure, City, and Country. These are high level entities to find out and understand the intersections of interoperability of smart city services. Each of the entities can be mapped with another and analysis can be made in the crossroads of this mapping. A set of dimensions have been chosen to give structure for analysis and design of smart city services. These dimensions are business, legal, usability, social and technical aspect.

In addition to the possible interoperability levels (service to service or mobile to user for instance) that need to be reached, other aspects (the eventual hierarchical relationship between entities for instance) must be taken into account. We believe that we need a more general framework that could identify these particular levels and deal with them. An evaluation system, so that already existing entities interactions can be analyzed in an efficient way or the conception of future services can be assessed, could be useful in this process.

III. Interoperability Framework

The goal of this section is to give a good intuition of what we intend by interoperability and how it fits in the SUS context. We will define the entities that are involved and their relationships. These relationships are those for which we would like to be able to talk about interoperability.

A. *Criteria*

Before defining the possible levels of interoperability, we must choose relevant evaluation criteria. Intuitively, the example of two possible actors, namely the service and the country, and the study of what the term suitability represents in their context is a first approach. The suitability of a service for a country means:

- the legal compatibility which includes the nature of the service and the type of data stored by the service (Example: the regulations regarding privacy differ from one country to the next).
- the social acceptability which takes into account the nature of the application that provides the service and the impact on persons (Example: using mobile phones in a kindergarten would probably not be well accepted in all countries)
- the localization capability with the language and the cultural references.

This first analysis suggests that the eligible elements, to 'measure' the interoperability, are the technical, the legal and the social details. A second analysis, regarding the services proposed in the SUS project and the interoperability issues that they raise, confirms that the previously presented criteria are to be taken into account. In addition, the nature of the SUS project, that connects academic and industrial partners, and its goals also lead us to highlight both the technological and commercial aspects of the interoperability evaluation. Then, because of the relevant elements (in our context) that our preliminary studies have identified, we choose to focus, as presented Fig. 1, on 4 specific points to analyze the relationship between two entities:

- the **technical issues** which correspond to the evaluation of available technologies (and their use) and to the communication standards both at hardware and software level
- the **legal issues** which are the consideration of laws and regulations that may impact on the entities
- the **usability/social acceptability issues** which target the cultural aspects as well as those related to the customization and the seamless use of a service regardless the environment
- the **business issues** which include, among other things, the business model that can be built and that could be convenient for the stakeholders

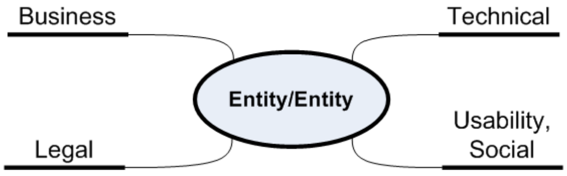


Figure 1: Dimensions of interoperability analysis

B. *Entities and Interoperability Matrix*

The concept of interoperability encompasses the relations that can exist between two or more entities. Then, the understanding of this concept requires prior knowledge of the behavior of entities in each specific case. Consequently, the study of interoperability within a well-defined ecosystem starts by the identification and the description of the involved entities. In the framework of the city services proposed in the context of the Smart Urban Spaces project, we have identified six main entities:

- the **mobile phone** which is the personal electronic device by means of which a person interacts with the (real or virtual) external environment. Note that this interaction can also be at the initiative of some external entity or the mobile phone itself and not necessarily its owner, who, in some cases, is perhaps not even aware an interaction took/is taking place.
- the **user** who corresponds to the person that will use a mobile phone to access the different proposed services
- the **infrastructure** which consists of either NFC readers, either contactless smart cards or tag systems that correspond to the 3 operating mode of NFC. In particular, a tag system is a system which manages the interface between a NFC-enabled device and a set of operations it is

willing to launch by means of reading a tag while a tag is a small piece of hardware (usually a plastic component with electrical circuits) that stores data accessible through the reader/writer NFC mode.

- the **service** which includes, in a particular field, a set of elementary operations to improve the daily lives of citizens (for instance a mobile ticketing service). The service takes generally the shape of an application running on a mobile phone
- the **city** represents the geographical area for which a range of services is offered to the citizens
- the **country** is the country where the city is located

Depending on the environment, several players of the same type can coexist and interact. Obviously, in a defined ecosystem, many mobile phones (belonging to many users) are activated as many services are offered to the citizens. Precisely, the possible interactions between these different actors allow defining the different levels of interoperability that can be achieved. For example, if we consider the case of two mobile phones that need to exchange some data, we will deal with potential hardware compatibility issues and communication standard problems.

	User	**Mobile**	**Infras.**	**Service**	**City**	**Country**
User						
Mobile						
Infras.						
Service						
City						
Country						

Figure 2: Interoperability matrix

Consequently, the study of relationships between each presented entity allows us to introduce the concept of 'Interoperability Matrix' (Fig. 2) to model the different possible levels of interoperability. Each cell represents the links that exist or can/should be tied. For example, the cell entity #1-entity #2 should be read as follows: what are the requirements for entity #1 to be 'interoperable' with entity #2? It should be noted that not all the cells play the same role regarding the notion of interoperability. This is explained in the following section.

IV. Resulting Evaluation Process

A. *Description*

The evaluation process can be used to describe/define requirements/interoperability for an entity over the other components of the ecosystem, for example a given service that must interact with the other actors (Mobile, User, etc.). The process, regarding two entities, is derived from a questionnaire that makes it possible to analyze the possible interactions in a cell of the interoperability matrix. The structure of the form can be decomposed into different blocks: a first part with general questions, a second part related to technical issues, a third block concerning legal aspects, a fourth part for the business related questions and finally a fifth part dealing with the usability/social acceptability elements. Thus, the stakeholders involved in the evaluation process correspond to the relations to analyze (cf. the general questions part of the forms).

The general part presents information (question to answer - who should fill this form - prerequisites) that help to explain and understand the context in which the analysis is performed. As for the other four parts, which correspond to the four dimensions of analysis, they each contain a set of questions to answer. These questions enable a detailed study of the elements that we find essential. It should be noted that these issues have only three possible answers, i.e., yes, no or maybe, to keep the process as simple as possible. ‘Maybe’ corresponds to a situation where the stakeholders are not sure about the answer to provide (for example because details are missing regarding a given entity or because the answer lies between yes and no).

From a practical point of view, the assessment is done by assigning a value to each answer. An answer ‘maybe’ is equivalent to 1 point, while the answers ‘yes’ or ‘no’ can both correspond to 0 or 2 points depending on their negative or positive nature concerning interoperability. For example, an answer ‘yes’ to the question ‘Can the Service be localized if required’ gives 2 points while a ‘yes’ to the question ‘Does the service make any country specific cultural reference’ gives 0 point. Then, for each category (technical, legal, business, usability/social acceptability), we define a percentage that is calculated as the ratio of the sum of the responses on the maximum (2 times the number of questions). This percentage represents in some way the degree of ‘interoperability’ achieved in the chosen dimension. In the previous example, assume that the answers to three questions in the Usability/Social category are respectively ‘yes’, ‘yes’ and maybe. The resulting percentage is therefore (0+2+1) / 6 or 50%.

Then, to graphically illustrate the set of results for an analysis of interactions between two entities, we use a Kiviat diagram. The diagram has four axes for each analysis dimension scaled from 0 to 100 (to represent the percentages). Depending on the references values which are used for the diagram (50 for each axis in our case, cf. Fig. 3), the results lead to a conclusion regarding the level of interoperability reached by the relation between two entities. This graphical representation also enables comparisons between different levels of interoperability (different types of relations in the interoperability matrix) or between different entities of the same nature.

B. *Application on a case*

We apply the Service to Country form to a real case to show its practical use. It represents the complete form for the Service to Country relation among the set of forms that must be built for each cell of the interoperability matrix. We first answer to the questions according to the four dimensions, then we calculate the percentages and finally, we draw the Kiviat diagram. In this example, the Service is the Daycare system and the Country is Finland. The form is presented Table I.

TABLE I. Service to Country form for Daycare and Finland

Daycare → Finland

Question to answer: What are the necessary conditions so that a given service can be used in my Country?
Who should fill this form: This form must be filled by a representative of a Country who is considering using a pre-existing Service, with the help of the Service provider.
Prerequisite(s): the country has rules and legislations for open data, privacy and security, and open interfaces of public information systems

Questions	Answers
Technical issues Can the Service be localized if required? Can the Service fit with the available hardware/software infrastructure available in my Country? Is the Service technology standard based?	Yes (2) Yes (2) Yes (2)
Legal issues Does the Service obey the specific regulations of my Country? Does the Service use and provide open public data as required by the regulations and contracts?	Yes (2) Maybe (1)
Business issues Will the benefit(s) gained by deploying the service be concrete? Is the cost/benefit ratio positive? Is it possible to use the same solution in many cities to save costs of public investment?	Yes (2) Yes (2) Yes (2)
Usability/Social questions Might the Service be subject to acceptation arguments in my Country? Can the Service be localized if required (note that this is also a technical issue)? Does the Service make any country specific cultural reference?	Yes (2) Maybe (1) Yes (0)

The results are presented in the Kiviat diagram Fig. 3. Globally, we can conclude that the Daycare reach a good level of interoperability at the Service to Country level in Finland.

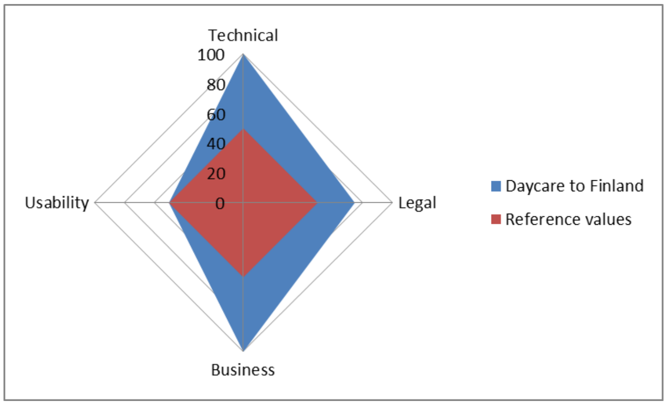


Figure 3: Daycare to Finland interoperability level analysis results

C. *First Contributions*

The first analysis and the initial feedback enable us to raise positive elements concerning the proposed interoperability evaluation process:

- Some partners of the SUS project started to use the first forms we have built as an evaluation tool for the services they have deployed, thus demonstrating it is a practical tool. The forms include quite simple questions (with yes/no/maybe answers) and the process (computation of the percentages for each category) that leads to the evaluation results is easy to achieve. By clearly identifying the forms to be filled on the basis of the interoperability aspects that are targeted, it is relatively easy to obtain a concrete result.
- The awareness of the possible problems is another positive element of the evaluation process. Indeed, the Kiviat diagram resulting from a form filling presents a clear view of the level of interoperability with respect to the reference values (namely the average values). In other words, the diagram allows pointing out the eventual strengths and weaknesses (of the evaluated interoperability relationship) according to the different criteria presented in the subsection 3.A. These eventual strengths and weaknesses are the points, with reference to the corresponding parts of the considered form, to take into account in the improvement of a given service.

V. Future Work

Obviously, to achieve the definition of the evaluation process, it is necessary to build a complete set of form mapping the cells of the matrix. Then, each cell of the matrix will be associated to a form whose structure will be the same as previously defined. This set of forms will not only provide guidance on services to be developed (before a concrete implementation), but also on improvements to existing services (to be deployed in other contexts).

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-324-7

Depending on the situation, it can be used by each player, by selecting the relevant elements to evaluate, to assess its level of interaction with external partners. These forms will provide a simple tool (questions with yes or no answers), flexible and including means for measuring (assessment model, Kiviat diagram) to focus on the dimensions of interoperability to enhance. The objective is to make it possible for the SUS project partners to use the complete tool and also to test it on more mobile contactless city services to obtain other valuable feedbacks. This set of forms has a dynamic aspect as it is built from exchanges between SUS partners and the experience gained during this project. It has an evolutionary shape and it also intended to be enriched by the experience feedbacks associated with its use.

VI. Conclusion

It is extremely difficult to take into consideration the entire elements which are essential to provide seamless services. Nevertheless, the experience of the SUS project has allowed us to understand and properly define the environment in which mobile contactless city services are expected to evolve. It helped us to identify the actors (User, Mobile, Infrastructure, Service, City and Country) which play a major role in this ecosystem. Based on this experience, our study on interoperability allowed us to specify the dimensions (technical, legal, business, usability/social) to consider while showing the possible interactions between entities in the interoperability matrix. We were able to present achievable levels of interoperability (represented by the cells of the matrix).

The consideration of these criteria and the interoperability framework that we have defined led us to initiate the implementation of an evaluation process based on a set of forms. This set, with elements structured according to the criteria defined above, contains forms that refer to the cells (levels) of the interoperability matrix. To deploy a seamless service, we must ensure to analyze its environment and the levels of compatibility (depending of the objectives) to reach. The set of forms provides tools to give a clearer view of the operating environment with a simple assessment model and to help achieve this goal. We were able to use the framework and a part of the forms on specific cases (the Daycare for instance) to show its relevance. Of course, we still need to complete this set of form and test it on another bunch of mobile contactless services.

Acknowledgment

This work was carried out within the framework of Smart Urban Spaces, an Information Technology for European Advancement (ITEA) project, the goal of which was to define new mobile e-services for cities. The proposed services mainly take advantage of specific technologies, in particular NFC, in order to ease the everyday life of European citizens. We would like to thank the partners of the Smart Urban Spaces project with whom we have been working. Open Europeans Sailing competition pilot was conducted by Forum Virium Helsinki, Bonwal, Helsinki race management, Helsinki Region Transport and Nokia. Authors wish to thank these parties for letting us use this pilot as an interoperability example.

We would also like to thank the University of Bordeaux which made possible, through its concrete support, the collaboration between VTT and LaBRI on this paper.

References

[1] B. Benyo, A. Vilmos, K. Kovacs, and L. Kutor. “NFC applications and business model of the ecosystem,” Presented at Mobile and Wireless Communications Summit, 2007. 16th IST. 2007.

[2] F. Borrego-Jaraba, I. Luque Ruiz, and M. A. Gómez-Nieto. “A NFC-based pervasive solution for city touristic surfing,” Personal and Ubiquitous Computing 15(7), 2011, pp. 731-742.

[3] Cityzi, Available: http://www.cityzi.fr [retrieved: January, 2014].

[4] V. Coskun, K. Ok, and B. Ozdenizci. “Near Field Communication: From Theory to Practice,” 2011.

[5] J. Fang, S. Hu, and Y. Han. “A service interoperability assessment model for service composition,” Proc. IEEE International Conference on Service Computing. 2004.

[6] Forum des services mobiles sans contact, “NFC mobile phones to benefit regions,” 2009. Available: http://www.nfc-forum.org/resources/white_papers/SMSC_liberty_equality_mobility.pdf

[7] Innovision Research and Technology, “Near field communication in the real world - turning the NFC promise into profitable, everyday applications,” 2007. Available: http://members.nfc-forum.org/resources/white_papers/Innovision_whitePaper2.pdf [retrieved: January, 2014].

[8] M. Isomursu, “Tags and the city,” PsychNology Journal 6(2), pp. 131-156. 2008.

[9] G. Madlmayr, “A mobile trusted computing architecture for a near field communication ecosystem,” Proc. of the 10th International Conference on Information Integration and Web-Based Applications & Services. 2008.

[10] G. Madlmayr, J. Langer, and J. Scharinger, “Managing an NFC ecosystem,” Proc. of the 7th International Conference of Mobile Business, 2008.

[11] O. Rouru-Kuivala, “NFC in urban settings,” in Touch the Future with Smart Touch, Espoo: VTT, 2009, pp. 171-173.

[12] J. Siden et al., “Home care with NFC sensors and a smart phone,” Proc. of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies. 2011.

[13] T. Tuikka and M. Isomursu, “Touch the Future with a Smart Touch”, 2009.

[14] P. Välkkynen et al., “A user interaction paradigm for physical browsing and near-object control based on tags,” Proc. Mobile HCI, Physical Interaction Workshop on Real World User Interfaces. Udine, Italy, 2003, pp. 31-34.

[15] P. Wegner, “Interoperability,” ACM Computing Surveys (CSUR) 28(1), 1996, pp. 285-287.

Economic View of Internet Freedom Issue

Rasim Alguliev
Department of information society problems
Institute of Information Technology of ANAS
Baku, Azerbaijan
rasim@science.az

Farhad Yusifov
Department of information society problems
Institute of Information Technology of ANAS
Baku, Azerbaijan
farhadyusifov@gmail.com

***Abstract*—In the present research, we examine the relationship between the Internet freedom and various social, political and especially economic factors, as they affect the Internet growth. The results show a strong relationship between a country's GDP and Internet penetration. In general, the hypothesis which predicts that the higher a country's GDP per capita, the more likely that it has Internet access and freedom, is supported.**

Keywords-Internet freedom; information environment; GDP; information security.

I. INTRODUCTION

Considering international experience, while researching philosophy of freedom, it is clear that Gross Domestic Product (GDP) per capita is much higher in countries with greater economic freedom [1][2][3]. More precisely, people have more economical freedom in the countries with high GDP. Per capita GDP is the value of all final goods and service produced within a country for domestic use and reserve, and it is considered as one of the main indicators of living standards of the country's population. Generally, Information and Communications Technology (ICT) policy of the country determines the basis of information freedom of the country. Information asymmetry problem existing on the Internet is viewed as one of the issues with a complex solution and deficiencies in this field are currently becoming more intensified.

In the research we examined, the relationship between the Internet development and various social, political and especially economic factors, as they affect the Internet growth. The results show that the Internet penetration is related to a country's wealth, per capita GDP, telecommunication infrastructure, urbanization and stability of the government.

Some views on information freedom are investigated and factors affecting Internet Freedom are analyzed and given correlation between volume of per capita GDP and number of Internet users.

II. SOME VIEWS ON INFORMATION FREEDOM

ICT and government policy of the country determine the quantity (and quality) of Information freedom. Although people's information freedom is declared as proclamatory, objective and subjective solution methods for its solution must be found in each country. This is directly connected to economic condition, regional position, political views, etc., of the country. For example, based on the statistical indicators, Internet access speed at 1Mb/sec per capita is considered as minimum for providing people's information freedom in Finland [4][5].

Information asymmetry problem existing on the Internet worldwide is viewed as one of the issues with a complex solution for provision of freedoms. High price factor of Internet can limit the people's ability to obtain information. In other words, people with Internet access can obtain more superior knowledge. Logically, it can cause formation of notions such as information monopoly, information dictatorship, information imperialism, etc.

Provision of freedoms, unwritten rules in existing environment, chaos, anarchy etc. can logically lead to formation of environment for prosperity of all kinds of crime. One of the most important issues for this stage is formation and development of information society.

Information environment – is such an environment, where information is created, stored, processed and transmitted. All forms of information exchange existing in the society are executed, and provide for existence and operation of the society as a single social organism. In general, information environment can be demonstrated as three integrants:

- Languages reflecting all forms of information on information relations occurring in the country;
- Content-volume, meaning and value (importance) of information;
- Information-communication infrastructure forming the material basis of information exchange.

It must be noted that, characteristics of contents and information-communication infrastructures define the information space of the country in total, as a whole.

The notion of information environment can concern the society as a whole, as well as any of its activity spheres. It can be noted that, information environment of science or its different fields (economy, culture and other information environments) can be discussed as information environment of the world, country, region and city.

Development of information environment in different countries happens irregularly within time and space, and depends of development level of the country. In modern society, information environment mainly has a network structure. The main connection form among points of information environments is Internet and it provides the technical means of information connection of one subject with another. From this standpoint, the Internet freedom

ISBN: 978-1-61208-324-7

problem is encountered as a component of freedoms provision and lately, existing problem has become more intensified. Development of legal basis of Internet is demonstrated as one of the relevant issues. Naturally, processes occurring in Internet environment cannot be regulated with existing laws. Freedoms of the users can be discussed based on the normative-legal basis to be created.

III. Factors Affecting Internet Freedom

Generally, there are objective and subjective factors affecting Internet freedom [6][7][8][9]. Absence of information resources in accordance with national standards, non-conduction of audit, absence of feedback mechanisms, and disinterestedness of the government in development of Internet can be sited as examples. Installation of different filters, analyzers within the borders of the country, total control of relations of users with Internet, limitation of access to web-sites and social networks are among the factors affecting Internet freedom.

Another important issue is the evident exaggeration of energy security problem of Internet lately. Thus, energy security problem, which is considered as one of main components of information security of the society, must be kept in focus constantly. As energy security is not a domestic issue of the government, it must be considered that, shut-down of a server located in a certain country limits the access possibility to existing information resources from other countries.

Artificial increase of Internet use prices, non-satisfactory services provided to the users by the providers, absence of formation of normal competition environment, etc., can be sited among factors affecting Internet freedom in developing countries [8][9][10][11].

In general, requirement of maximum Internet freedom in countries with poorly developing economy does not reflect existing reality. From this standpoint, a system of indicators characterizing the economic potential of the country must be developed considering economical potential of the country. For example, countries can be classified and divided in classes by regions, based on per capita Internet speed in the country. Surely, this evaluation is connected to a certain period. Because with passage of time, economic conditions of the countries change, to be more precise, Internet capabilities change. Thus, geographical landscape of Internet freedom in world countries, and regions can be obtained.

IV. Correlation Between Volume of Per Capita GDP and Number of Internet Users

Slow development of information technologies, and limited or no Internet access opportunities in developing countries are justified by a number of reasons:

- Low level of income limits the Internet access and in general, use of capabilities of modern technologies by population and companies.
- Absence of the desired level of infrastructure in cities and territories, as well as low number (density) of potential consumers leads to further increasing expenses on development of infrastructure;
- Poor development of infrastructure and very limited access opportunities to them results in high prices of Internet access;
- Low level of literacy of population, non-sufficient level of computer knowledge;
- Unformed or non-existent normative-legal base.

According to the research, economic indicators of the country and difference among them are regarded as one of the most evident factors [10][11][12][13]. Volume of per capita GDP determines the capabilities of citizens and companies as potential consumers on the Internet market. Share of Internet users among population increases as these indicators increase. Besides, there are relevantly more Internet users in countries with high or very high GDP per capita. We can distinctly see this tendency as we look at the correlation (in Fig.1) between GDP volume per capita and ratio of Internet users (I_{users}) and the base population (P) in Azerbaijan in 2002-2010 years [14].

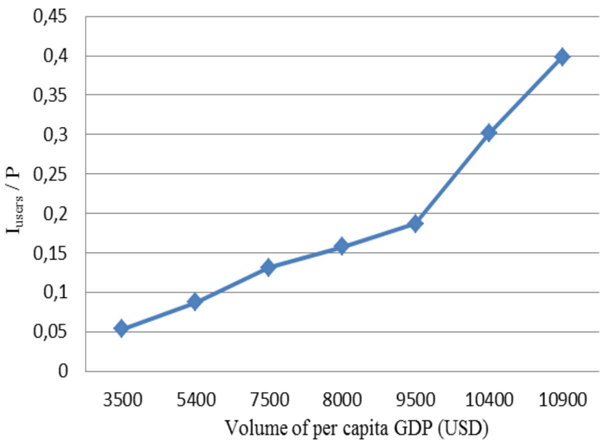


Figure 1. Correlation between GDP volume per capita and ratio of Internet users (I_{users}) and the base population (P) in The Republic of Azerbaijan in 2002-2010 years.

The results show a strong relationship between a country’s GDP and Internet penetration. Developed countries tend to boast a higher Internet penetration rate than poor countries. In other words, countries with low GDP per capita are all on the low end of the Internet penetration rate. In generally, hypothesis which predicts that the higher a country’s GDP per capita, the more likely that it has Internet access, is supported. In this case, to a certain extent, Internet development is more likely to be affected by economic factors rather than social and political factors.

In other words, GDP per capita is considered as one of the main indicators of living standards of country’s population. If the volume of GDP per capita is high, then population of that country has more economic freedom. Provision of economic freedom means capability to access Internet, and in this case, we can talk about provision of Internet freedom. It must be noted that, the factors affecting Internet development process are not of linear character. Effect of economic factors is formed at a certain chronological stage or depending on a sequence of different effects.

V. Conclusion

Volume of per capita GDP is accepted as one of the main indicators of living standards of a country's population. Volume of per capita GDP determines the potential consumer capabilities of citizens on Internet market. Increase of these indicators leads to increase of Internet users' share among population. This suggests that provision of Internet freedom depends on economical factors and conduction of researches in this field is necessary.

References

[1] A. B. Kim, "Advancing Freedom: The Path to Greater Development and Progress," www.heritage.org, [retrieved: January, 2014].

[2] J. Gwartney, R. Lawson, and J. Hall, 2012 Index of Economic Freedom, www.heritage.org, [retrieved: January, 2014].

[3] J. Gwartney, R. Lawson, and J. Hall, Economic Freedom of the World: 2013 Annual Report, www.freetheworld.com, [retrieved: February, 2014].

[4] Broadband now a legal right in Finland, www.itu.int, [retrieved: February, 2014].

[5] Making broadband available to everyone. The national plan of action to improve the infrastructure of the information society, www.lvm.fi, [retrieved: February, 2014].

[6] D.V. Zakharchenko, "Internet-technologies as development factor of infrastructure of modern economy," Economy and Management, no. 5, vol. 78, 2011, pp 122-125. http://ecsocman.hse.ru, [retrieved: February, 2014].

[7] T.V. Maksiyanova, "Influence of Internet-economy of GDP of Russia", 2012, http://vernadsky.tstu.ru, [retrieved: January, 2014].

[8] L. Andres, D. Cuberes, M. Diouf, and T. Serebrinsky, "The diffusion of the Internet: A cross-country analysis," Telecommunications Policy, no. 34, vol. 5-6, 2010, pp. 323-340.

[9] H. Xiaoming and C. S. Kay, "Factors affecting Internet development: An Asian survey," First Monday, vol. 9, no. 2, 2004, http://firstmonday.org, [retrieved: February, 2014].

[10] S. Johnson, J. A. Robinson, and P. Yared, Income and Democracy, 2008, www0.gsb.columbia.edu, [retrieved: January, 2014].

[11] Freedom on the Net 2013, A Global assessment of Internet and Digital media, Full Report, www.freedomhouse.org, [retrieved: January, 2014].

[12] S. Amiri, and B. Reif, "Internet Penetration and its Correlation to Gross Domestic Product: An Analysis of the Nordic Countries, International Journal of Business", Humanities and Technology, no. 2, vol. 3, 2013, pp. 50-60.

[13] Internet World Stats: Countries with Highest Internet Penetration Rates, http://www.internetworldstats.com/top25.htm, [retrieved: February, 2014].

[14] Country profile statistics, www.indexmundi.com, [retrieved: February, 2014].

Usability Evaluations for Everybody, Everywhere:

A field study on Remote Synchronous Testing in Realistic Development Contexts

Fulvio Lizano
Department of Computer Science
Aalborg University
Aalborg, Denmark
fulvio@cs.aau.dk

Jan Stage
Department of Computer Science
Aalborg University
Aalborg, Denmark
fulvio@cs.aau.dk

***Abstract*—Although Human-Computer Interaction (HCI) techniques, as usability evaluations, are considered strategic in software development, there are diverse economic and practical constraints in their application. The integration of these tests into software projects must consider practical and cost-effective methods such as, for instance, the remote synchronous testing method. This paper presents results from a field study in which we compared this method with the classic laboratory-based think-aloud method in a realistic software development context. Our interest in this study was to explore the performance of the remote synchronous testing method in a realistic context. The results show that the remote synchronous testing method allows the identification of a similar number of usability problems achieved by conventional methods at a usability lab. Additionally, the time spent using remote synchronous testing is significantly less. Results obtained in this study also allowed us to infer that, by using the remote synchronous testing method, it is possible to handle some practical constraints that limit the integration of usability evaluations into software development projects. In this sense, the relevance of the paper is based on the positively impact that remote synchronous testing could have in the digital accessibility of the software, by allowing extensive use of usability evaluation practices into software development projects.**

Keywords-Usability evaluations; remote synchronous testing method; integration of usability evaluation in software development projects; field study.

I. INTRODUCTION

Usability has a significant impact on software development projects [15]. Common usability activities, as usability evaluations, are relevant and strategic in diverse contexts (e.g., organizations, software development process, software developers and users) [3], [13].

However, economic and practical issues limit integration of usability evaluations into software projects, where limited schedules and high expectations of stakeholders to obtain effective/efficient results faster, are common. Productivity has been a recurrent concern in the industry [5], [12] and is something that makes it very difficult to justify some HCI activities [20].

Bearing this in mind, any effort to integrate usability evaluations into software projects must necessarily consider practical and cost-effective methods, such as the remote synchronous test.

In this paper, we present the results of a field study that aimed to compare the remote synchronous test method against the classic laboratory-based think-aloud method in a realistic software development context.

In the following section, we offer an overview of related works. The next section presents the method used in our research. Following this, we present the results of our study. After the results are summarized, the paper presents the analysis before concluding with suggestions for future work.

II. RELATED WORKS

Integration efforts of usability evaluations into software projects have economic and practical constraints.

High consumption of resources in usability evaluations is a recurrent perception in diverse contexts [2], [3], [19], [22], [23]. This fact could explain why usability has a lower valuation for the organization's top management [8], becoming manifest by the lack of respect and support for usability and the HCI practitioners [9]. Therefore, cost-justification of usability may be difficult for many companies when it is perceived as an extra cost or feature [20].

On the other hand, three of the most cited practical constraints are related to: the difference of perspectives between HCI and Software Engineering (SE) practitioners, the absence or diversity of methods and, finally, the users' participation.

The first constraint related to the difference of perspectives between HCI and SE practitioners is contextualized in the difference of opinions they have about what is important in software development [17]. This diversity of perspectives results in contradictory points of view regarding how usability testing should be conducted and is something that may result in a certain lack of collaboration between HCI and SE practitioners. It is possible to find the origin of this discrepancy between these two perspectives in the foundations of the HCI and SE fields. Usability is focused on how the user will work with the software, whereas the development of that software is centered on how the software should be developed in a practical an economical way [27]. These conflicting perspectives result in tensions between software developers and HCI practitioners [18], [27].

ISBN: 978-1-61208-324-7

The second constraint relates to the absence or diversity of methods, and has two opposing views. Firstly, some researchers report a lack of appropriate methods for usability evaluation [2], [19] or a lack of formal application of HCI and SE methods [15]. This situation may explain why the UCD community has expressed criticism about the real application of some software development principles [25]. Secondly, it is reported that the existence of numerous and varied techniques and methodologies in the HCI and SE fields could hamper the integration [18].

Finally, the participation of customers and users has become another relevant limitation for the integration of usability evaluations into software projects [2], [3], [19]. This matter is a permanent challenge to the dynamic of the software development process. Users and customers have their own problems and time limitations, and these normally limit their participation in software development activities such as usability evaluations.

The literature reported different proposals for handling the aforementioned three practical constraints. Firstly, in the case of the difference of perspectives between HCI and SE practitioners, some studies have suggested that increased participation of developers in usability testing could positively impact their valuation of usability [13]. This improvement in the developers' perspectives could make them more conscious of the relevance of HCI techniques.

Secondly, with respect to the absence or diversity of methods, an integration approach based on international standards is proposed [7] in order to enable consistency, repeatability of process, independence of organizations, quality, etc. A similar approach suggests the integration of HCI activities into software projects by using SE terminology for HCI activities [6].

Finally, regarding the constraint related to the participation of customers and users, some researchers have suggested several practical actions (e.g., smaller tests in iterative software development processes, testing only some parts of the software, and using smaller groups of 1–2 users in each usability evaluation [14].

These aforementioned studies were conducted on limited realistic contexts, e.g., literature reviews [7], [20], [23], [25], [27], surveys [2], [5,], [9], [15], [19], experiments in labs [22], [26] and case studies [13], [18]. Other papers cited above present proposals of projects or methods [6], [8], [17]. There are only three studies with a more empirical base in more realistic contexts [4], [13], [14]. Confidence in the results of these studies should be improved by other studies made in a realistic development context.

III. METHOD

We have conducted an empirical study aimed at comparing the remote synchronous testing method (condition R) with the classic laboratory-based think-aloud method (condition L).

By using remote synchronous testing, the test is conducted in real time, but the evaluators are separated spatially from the users [1]. The interaction between the evaluators and the users is similar to those at a usability lab. There are many studies that confirm the feasibility of remote usability testing methods [1], [10], [28]. Actually, there is a clear consensus regarding the benefits obtained by using this method (e.g., no geographical constraints, cost efficiency, access to a more diverse pool of users and similar results as a conventional usability test in a lab) [1], [24]. The main disadvantages are related to problems of generating enough trust between the test monitor and users, a longer setup time, and difficulties in re-establishing the test environment if there is a problem with the hardware or software [1].

Three usability evaluations were made by three teams using a classic usability lab. In addition, another three usability evaluations were conducted by another three teams using a remote synchronous testing method.

All of these teams were formed by final-year students of SE who had 18 months of practical experience working in software development. This experience is the result of an academic project created by the students by developing a software system in a real organization.

A. Participants

In order to be considered for our research, the software projects must meet our requirements regarding users being available for the tests. Considering these criteria, 16 of 30 teams, and their software projects, were pre-selected as potential participants in the experiment. Finally, we randomly selected six teams who were randomly distributed throughout the R and L conditions.

The teams were formed by final-year students who were finishing their last course in System Engineering. These participants were organized into six teams consisting of three members each. A total of 18 people participated in our study. The average age was 22 (SD=2.13) and 17% were female. In addition to the courses taken previously, the participants had amassed nearly 18 months of real experience of practical academic activity by developing a software system in a real organization that sponsored the project. These organizations provided regular assessments and formal acceptance (or rejection) of the software. Several users and stakeholders were also involved in the process. The scope of the software projects was carefully controlled in order to guarantee a similar level of effort from all of the participants. The average of the final assessment of the project was 9.67 on a scale of 1–10 (SD=0.33). As an incentive for participation, the participants received extra credits. The conditions, code, members and software are presented in Table I.

B. Training and advice

All participants received training and advice during the experiments (remotely for R condition). In the training, we presented and explained several forms and guidelines based on commonly used theories [16], [24]. In addition, a workshop was made in order to putting into practice the contents of the training materials. The participants received specific instructions in order to consider three categories of usability problems: critical, serious, and cosmetic [1]. The number of hours spent in training was 10 (four hours in lectures and six hours in practice). Furthermore, the advice provided to the participants included practical issues concerning how to plan and conduct usability evaluations.

TABLE I. TEAMS, MEMBERS, AND STAFF FOR THE USABILITY EVALUATION

Cond.	Code	Members	Software
L	L1	3 males	Students' records in a private college
	L2	1 female, 2 males	Internal postal management system in a financial department of a public university
	L3	1 female, 2 males	Laboratory equipment management in a biological research center belonging to a public university
R	R1	1 female, 2 males	Criminal record in a small municipal police station
	R2	3 males	Management of documents related to general procurement contracts in an official national emergency office
	R3	3 males	Students' records in a public school

TABLE II. PROBLEMS IDENTIFIED PER TYPE OF PROBLEM. (%)= PERCENTAGE PER CONDITION.

Cond.-> Problems	L	R
Critical	36 (52%)	33 (56%)
Serious	29 (42%)	22 (37%)
Cosmetic	4 (6%)	4 (7%)
Total	69	59

C. Procedure

The design of the experiment increased confidence in the results and objectivity of the development teams during the evaluation process. Under the two conditions, each team had to test the software system made by another team, who also tested another software system made by a third team.

Each test had two main parts. The first part, under the responsibility of the team who made the software, corresponded to the planning of the complete process (e.g., planning, checklists, forms, coordination with users, general logistics, etc.). The planning included a session script with 10 potential tasks of the software.

In the second part of the tests, another team conducted the sessions with the users. The test monitor of this team had to select, for each user, five tasks from those previously defined. We thought this measure would increase the impartiality of the process; the developers of the software could not interfere in the selection of the task and the users had to work with different tasks in each session. Next, the test monitor guided the users in the development of the task while the logger and the observers took notes. The test ended with a final analysis session conducted by a facilitator [16].

D. Settings

The test conducted under the L condition used a state-of-the-art usability lab and think-aloud protocol [21], [24]. Each test included three sessions where the users were sat in front of the computer and the test monitor was sat next the users. The logger and observers were present in the same room. In the case of the R condition, the tests were based on the remote synchronous testing [1]. All participants were spatially separated. Users were in the sponsors' facilities. Each test included three sessions with users.

E. Data collection and analysis

Each user session was video recorded. The video included the software session recorder (video capture of screen) and a small video image of the user. Under R conditions, the video also recorded the image of the test monitor. We also used a test log to register the main data of each activity (i.e., date, participant, role, activity and time consumed) and the usability problem reports.

The data analysis was conducted by the authors of this paper based on all data collected during the tests. The tests produced six sets of data for analysis, i.e., six usability problem reports, six test logs and six videos.

The consistency of the classification of the usability problems by participants was one of the main concerns in this study. Consequently, our analysis included an assessment of such classification. Our intention was to be sure that this classification was done consistently according to the instructions given to all participants during the training. We assessed the problem categorization by checking the software directly in order to confirm the categorization given by participants to a usability problem. The videos were thoroughly walked through in order to confirm this categorization.

The tests were conducted on different software systems. There is not a joint list of usability problems. This is the reason why, in our analysis, we compared the differences between both conditions by using average and standard deviations calculated separately for each condition.

Using the test logs, we analyzed the time spent in all the tests. We considered individual and group time consumption. We calculated totals, averages and percentages to facilitate the analysis. We included in this process all the activities made by all members of the teams in the preparation of the test (e.g., usability plan, usability tasks, etc.) and the conducting of the test itself. In the analysis, we also considered other participants, such as the users and observers, in order to consider a more realistic context.

Finally, in order to identify significant differences in the data collected, we used independent-sample t tests.

IV. RESULTS

A. Problems identified per type

Table II shows an overview of the usability problems identified under the two conditions. The problems are classified by their type. The largest number of problems was critical. The lowest number of problems identified was in the category of cosmetic problems. The distribution of all types of problems, among the two conditions, was relatively uniform. An independent-sample t test for the number of usability problems identified for the three categories, under both conditions, showed no significant difference (p=0.404). The fact that there are no significant differences between the

TABLE III. USERS' TASKS COMPLETION TIME AND TIME PER PROBLEM. UP= TOTAL NUMBER OF USABILITY PROBLEMS IDENTIFED PER CONDITION

Condition-> Test–User	**L (UP 69)**		**R (UP 59)**	
	Tot. Minutes	**Avg. per task (SD)**	**Tot. Minutes**	**Avg. per task (SD)**
T1–U1	10.8	2.2 (1.9)	30.0	6.0 (1.3)
T1–U2	9.7	1.9 (1.0)	18.3	3.7 (1.6)
T1–U3	12.8	2.6 (2.5)	18.7	3.7 (1.6)
T2–U1	6.1	1.2 (0.4)	17.6	3.5 (1.8)
T2–U2	14.3	2.9 (0.8)	13.3	2.7 (1.3)
T2–U3	8.4	1.7 (0.7)	8.9	1.8 (0.7)
T3–U1	7.4	1.5 (1.0)	11.2	2.2 (2.4)
T3–U2	6.9	1.4 (0.9)	9.0	1.8 (1.4)
T3–U3	11.1	2.2 (1.1)	10.5	2.1 (2.1)
Total Avg. por task (SD)	87.6 1.94 (0.5)		137.4 3.10 (1.3)	
Avg. task completion time per problem, in minutes	1.26		2.32	

L and R conditions is a reflection of the similarity of the effectiveness of these methods in terms of the number of problems identified.

B. *Task completion time*

The task completion time was less in the tests made under the L condition. In these tests, the users spent a total of 87.6 minutes completing the five tasks assigned to each one. The average time per user/task was 1.94 (SD=0.5). The average task completion time per usability problem identified under the L condition was 1.26. In the tests made under the R condition, the task completion time was 137.4, the average time per user/task was 3.10 (SD=1.3), and the average task completion time per problem was 2.32. In Table III, we present these results.

An independent-sample t test for the task completion time of the nine users considered under the two conditions showed a significant difference (p=0.018).

The analysis of the videos recorded during the tests made under the R condition showed delays due to technical problems – mainly in the communication between the actors (i.e., users, test monitor, technician, etc.). In addition, in general, the users in their normal jobs were more distracted. On the contrary, in the case of the tests made at the laboratory, the users were more focused, and the guidance of the test monitors was more effective.

C. *Time spent in the tests*

The time spent to complete the tests presents an entirely different perspective to that shown in the previous section. Here, the tests conducted under the R condition consumed less time than that conducted under the L condition.

TABLE IV. TIME SPENT IN THE TESTS. UP= TOTAL NUMBER OF USABILITY PROBLEMS IDENTIFIED PER CONDITION

Condition-> Activity	**L (UP 69)**	**R (UP 59)**
Preparation	2500 (102)	1580 (123)
Conducting test	1320 (73)	840 (42)
Analysis	980 (157)	710 (71)
Moving staff/users	1110 (107)	160 (57)
Tot.time spent per test	5910 (220.5)	3290 (102)
Avg. time per problem in minutes	85.7	55.8

In Table IV, we presented an overview of the time spent in the tests conducted under the two conditions. This table includes the average number of minutes spent on test activities. The standard deviation is shown between parentheses. At the end, the table also shows the average of time per problem in minutes.

These results included all the actors involved in the tests (i.e., users, test monitor, logger, observers, etc.). In this sense, it is possible to consider these results more realistic; here, all of the elements/persons required to perform the tests are included. An independent-sample t test, for the average time spent in the tests, for both conditions, showed an extremely significant difference ($p<0.001$).

The time spent on each activity during the tests confirms these extremely significant differences for all of the activities – except in the analysis. In preparation, conducting the tests, and moving staff, the independent-sample t tests for the time spent in the three tests conducted under each condition, showed extremely significant differences ($p<0.001$ for all of the cases). In the case of the analysis, the difference was significant ($P=0.045$).

V. DISCUSSION

Usability evaluations made by using the remote synchronous testing method are a cost-effective alternative to integrating usability evaluations into software projects. The number of usability problems identified by this method is similar to that obtained by conventional tests made in a usability laboratory. Additionally, there is a significant difference between the time spent on the remote synchronous test method and that spent on the tests made in the lab.

We confirmed the feasibility of conducting usability evaluations by software developers using diverse methods, including the remote synchronous testing method [4], [11], [26]. In addition, we also confirmed the similarity to the number of problems identified by the conventional lab method [1]. However, in the case of the time spent, our results differ from those of others [1] who argue that the time spent to conduct tests by using lab and remote synchronous tests was quite similar. In our case, the difference in time consumption for both methods was significantly favorable in the remote synchronous testing method. A detailed analysis of the test logs showed us that, in the tests made under the L condition, the logistic matters consumed much more time than in the tests under the R condition. Considering our aim of confirming previous findings in a realistic development context, logistic matters must be considered as factual components of any usability test.

The analysis of the procedures followed the conducting of the tests (reported in the usability problem reports) and the test logs showed that, by using the remote synchronous testing method, it is possible to achieve several practical advantages that save time in the tests.

It is possible to contextualize these advantages in the results of the time spent on the tests' activities shown in Table IV. Firstly, in the case of the preparation activities, the virtualization of the complete coordination process saved time and effort. The coordination between teams and other actors was easier and more efficient by using email, chat, video conferences, etc.

Secondly, in the activities of conducting the tests it was also easy and efficient to use all the software tools used during the tests. Even when considering that the task completion time was shown to be better in the tests made under the L condition (see Table III), differences in the overall process were evident due to this task completion time only being related to the time spent by users to complete the tasks. On the contrary, in the conducting activities of the tests, all of the elements and actors required to conduct the whole test are included (i.e., users, test monitor, logger, observers, etc.)

Thirdly, the difference in the analysis was also significant due to the technological tools that facilitated the conducting of the analysis sessions by the facilitator. In a certain way, the videos also showed that the virtualization of the process seems to produce a shared feeling about the relevance of productivity during the virtual sessions.

Finally, the results in the moving activities explain themselves. In the realistic development context used in this study, it is clear that avoiding the movement of the usability evaluation staff is one of the most relevant advantages in terms of time consumption.

In general, all of the advantages of the remote synchronous test cited in the literature were confirmed in the realistic contexts considered in our study [1], [24]. In the case of the disadvantages, we could only identify – in the analysis of the test logs – some problems in the setting of the hardware and software tools used in the process [1].

At this point in the discussion, the economic advantages of the remote synchronous testing method become evident. Furthermore, this method also helps to handle other practical problems of the integration of usability evaluations into software projects.

In our study, we have also confirmed the feasibility of the active participation of software developers in usability evaluations [4], [13], [26]. The participants played several roles in the usability evaluation teams (e.g., test monitor, logger, observer and technician). This confirmation is relevant when considering the context used in our study (i.e., lab and remote synchronous tests under more realistic conditions). The design of our experiment proved to be very useful because all of the teams actively participated in all of the process (i.e., planning and conducting of the test) and with impartiality. It is a fact that these levels of participation of developers in usability evaluations may impact positively upon their perspective regarding usability and the HCI practitioners [17] and will reduce the tensions between SE and HCI practitioners [18], [27].

Furthermore, in the case of the problem related to the lack of formal application of HCI techniques, our experiment found that by using guidelines and basic training, it is possible to prepare developers for conducting usability evaluations. In a certain way, the theory used to inspire the guidelines used in the tests has followed the suggested approach [7] of using standards to help the integration of usability evaluation into software projects. The analysis of the dynamic of the tests registered in the videos did not show any particular significant problems.

In the case of the tests made by using the remote synchronous testing method, the guidelines were fundamental in conducting the remote process. Considering the similarity of the results in the remote synchronous tests and those obtained in the lab, it is clear that the guidelines served their purpose.

Considering these facts, we can conclude that, by using guidelines based on standards, it is possible to improve the perception of the lack of appropriate methods for usability evaluation [2], [19].

Finally, our study also found that the reported problem [2], [3], [19] relating to the participation of customers and users can be handled well by using the remote synchronous testing method. The users do not need to drastically change their activities. Certainly, the task completion time was higher in the remote synchronous testing method but, putting this element in perspective for the whole process, it is always possible to see the strengths of the remote synchronous testing method. Furthermore, other actors did not have to go to the lab.

VI. CONCLUSSION

In this paper, we presented results of a study aimed to compare the remote synchronous test method against the classical laboratory-based think-aloud method in a realistic software development context. Several tests were conducted by final-year students who had 18 months of practical experience. Although the tests were made on software systems for different organizations and purposes, the scope of these software systems was carefully controlled in order to provide similar settings for the study.

The identification of a similar number of usability problems and lower time consumption, make of Remote Synchronous a good alternative for integrating usability evaluations into software projects. By using this method it is possible to involve more software developers into the conduction of usability testing. Such aim only requires basic training, guidelines and essential advice. Basic guidelines and training allows handling the problems related to the methods. Finally, one of the most relevant advantages of this method is to facilitate the participation of users, developers and other potential actors in the tests. By avoiding unnecessary movements of these persons, their participation will be easily justified

Our study has two main limitations. Firstly, the participants in the study were final-year undergraduate students. Nevertheless, the real conditions present in our study have allowed for a control of this bias. Secondly, we used only two usability evaluation techniques. However, our selection considered an ideal benchmark of high interaction with users (lab) and the alternative option which was the focus of our study. In our study, we were focused on the problems identified and the time consumption metrics in a realistic development context. For future work, it is suggested that, for the same context, a deeper analysis of other metrics, such as the improvement of the perspective of software developers regarding usability – which is another expected result of close participation of developers in usability evaluations – should be conducted.

ACKNOWLEDGMENT

The research behind this paper was partly financed by UNA, MICIT, CONICIT (Costa Rica), and the Danish Research Councils (grant number 09-065143). We are very grateful to the participants, observers, facilitators, organizations and users that helped us in this research.

REFERENCES

[1] M.S. Andreasen, H.V. Nielsen, S.O. Schrøder, and J. Stage, “What happened to remote usability testing?: an empirical study of three methods,” Proc. SIGCHI, ACM Press, 2007, pp. 1405-1414.

[2] C. Ardito et al., “Usability Evaluation: a survey of software development organizations,” Proc. 33 International Conference on Software Engineering & Knowledge Engineering, 2011. Pp. 282-287.

[3] J.O. Bak, K. Nguten, P. Risgaard, and J. Stage, “Obstacles to Usability Evaluation in Practice: A Survey of Software Development Organizations,” Proc. NordiCHI, ACM Press, 2008, pp.23-32.

[4] A. Bruun and J. Stage, “Training software development practitioners in usability testing: an assessment acceptance and prioritization,” Proc. OzCHI, ACM Press, 2012,pp.52-60.

[5] P.F. Drucker, “Knowledge-Worker Productivity: The Biggest Challenge,” in California management review,41(2), 1999, pp.79-94.

[6] X. Ferré, N. Juristo, and A. Moreno, “Which, When and How Usability Techniques and Activities Should be Integrated,” in Human-Centered Software Engineering - Integrating Usability in the Software Development Lifecycle, Springer Netherlands, 2005, pp. 173-200.

[7] H. Fischer, “Integrating usability engineering in the software development lifecycle based on international standards,” Proc. SIGCHI symposium on Engineering interactive computing systems, ACM Press, June 2012, pp. 321-324.

[8] T. Granollers, J. Lorés, and F. Perdrix, “Usability engineering process model. Integration with software engineering,” Proc. HCI International, 2003, pp 965-969.

[9] J. Gulliksen, I. Boivie, J. Persson, A. Hektor, and L. Herulf, “Making a difference: a survey of the usability profession in Sweden,” Proc. NordiCHI, ACM press, 2004, pp. 207-215.

[10] M. Hammontree, P. Weiler, and N. Nayak, “Remote usability testing,” in Interactions, 1, 3, 1994, pp. 21-25.

[11] H.R. Hartson, J.C. Castillo, J. Kelso, and W.C. Neale, “Remote evaluation: The network as an extension of the usability laboratory,” Proc. CHI, ACM Press, 1996, pp. 228-235.

[12] A. Hernandez-Lopez, R. Colomo-Palacios, and A. Garcia-Crespo, “Productivity in software engineering: A study of its meanings for practitioners: Understanding the concept under their standpoint,” Proc. Information Systems and Technologies (CISTI), IEEE Press, June 2012, pp. 1-6.

[13] R.T. Hoegh, C.M. Nielsen, M. Overgaard, M.B. Pedersen, and J. Stage, “The impact of usability reports and user test observations on developers' understanding of usability data: An exploratory study,” in International journal of Human-Computer Interaction, 21(2), 2006, pp. 173-196.

[14] Z. Hussain et al., “Practical Usability in XP Software Development Processes,” in Proc. ACHI, January 2012, pp. 208-217.

[15] Y. Jia, “Examining Usability Activities in Scrum Projects–A Survey Study,” Doctoral dissertation, Uppsala Univ., 2012.

[16] J. Kjeldskov, M.B. Skov, and J. Stage, “Instant data analysis: conducting usability evaluations in a day,” Proc. NordiCHI, ACM Press, 2004, pp. 233-240.

[17] J.C. Lee, “Embracing agile development of usable software systems,” In Proc.CHI'06 extended abstracts, ACM Press, 2006, pp. 1767-1770.

[18] J.C. Lee and D.S. McCrickard, “Towards extreme (ly) usable software: Exploring tensions between usability and agile software development,” in Proc. Agile Conference (AGILE), IEEE Press, August 2007, pp. 59-71.

[19] F. Lizano, M.M. Sandoval, A. Bruun, and J. Stage, “Usability Evaluation in a Digitally Emerging Country: A Survey Study,” Proc. INTERACT, Springer Berlin Heidelberg, 2013, pp. 298-305.

[20] G.H. Meiselwitz, B. Wentz, and J. Lazar, Universal Usability: Past, Present, and Future, Now Publishers Inc., 2010.

[21] J. Nielsen, Usability engineering, Morgan Kaufmann Publishers, 1993.

[22] J. Nielsen, “Guerrilla HCI: Using discount usability engineering to penetrate the intimidation barrier,” in Cost-justifying usability, 1994, pp. 245-272.

[23] D. Nichols and M. Twidale, “The usability of open source software,” in First Monday, 8(1), [online], Available: http://firstmonday.org/ojs/index.php/fm/article/view/1018/939 , [retrieved: 01, 2014], 2003

[24] J. Rubin and D. Chisnell, Handbook of usability testing: how to plan, design and conduct effective tests, John Wiley & Sons, 2008.

[25] A. Seffah, M.C. Desmarais, and E. Metzker, “HCI, Usability and Software Engineering Integration: Present and Future,” In Human-Centered Software Engineering, Seffah, A. et al. (eds.), Springer: Berlin, Germany, 2005.

[26] M.B. Skov and J. Stage, “Training software developers and designers to conduct usability evaluations,” in Behaviour & Information Technology, 31(4), 2012, pp. 425-435.

[27] O. Sohaib and K. Khan, “Integrating usability engineering and agile software development: A literature review,” Proc. ICCDA, IEEE Press, 2010, vol. 2, pp. V2-32

[28] K.E. Thompson, E.P. Rozanski, and A.R. Haake, “Here, there, anywhere: Remote usability testing that works,” Proc. Conference on Information Technology Education, ACM Press, 2004, pp. 132–137.

Characterization of Real Internet Paths by Means of Packet Loss Analysis

Luis Sequeira, Julián Fernández-Navajas, Jose Saldana
Communications Technology Group (GTC)-Aragón Inst. of Engeneering Research (I3A)
Dpt. IEC. Ada Byron Building. EINA Univ. Zaragoza
Zaragoza, Spain
Email: {sequeira, navajas, jsaldana}@unizar.es

***Abstract*—The behaviour of the routers' buffer may affect the Quality of Service (QoS) of network services under certain conditions, since it may modify some traffic characteristics, as delay or jitter, and may also drop packets. As a consequence, the characterization of the buffer is interesting, especially when multimedia flows are transmitted and even more if they transport information with real-time requirements. This work presents a packet loss analysis with the aim of determining the technical and functional characteristics of the real buffers (as, e.g., behaviour, size, limits, input and output rate) of a network path. An improved methodology is considered in which two different buffers are concatenated. It permits the estimation of some parameters of the intermediate buffers (size, input and output rate) in a network path including different devices across the Internet. The method presented in this paper permits the characterization of commercial router buffer by means of the analysis of the dropped packets in the buffer.**

Keywords-Buffer size; queueing; unattended measurements.

I. Introduction

The number of users of multimedia services (e.g., videoconferencing and Voice over IP, VoIP) grows every day and they generate an increasingly significant amount of traffic over the Internet. At the same time, users demand a good experience with these services. In this context, Internet Service Providers (ISP's) have to grant a high performance network with a certain degree of Quality of Service (QoS), especially when the access networks have to support to real-time applications.

Traditionally, the available bandwidth between two end-to-end devices has been used as a parameter that can give a rough idea of the expected quality. But nowadays, we know that QoS is also affected by the behaviour of the intermediate buffers, which is mainly determined by their size and their management policies. As it was observed in [1], the policies implemented by the router buffer may cause different packet loss behaviour, and may also modify the quality of the service (VoIP in that case, measured in terms of R-factor, Transmission Rating Factor). The influence of the router buffer on another real-time service (i.e., an online game) was studied in [2], showing the mutual relationship between the size and policies of the buffer, and the obtained subjective quality, which mainly depends on delay and jitter in this case. The results show that small buffers present better characteristics for maintaining delay and jitter in adequate levels, at the cost of increasing packet loss. In addition, buffers whose size is measured in packets also increase packets loss.

Many access network devices are designed for big packets, typical of services requiring bulk data transfers [3], such as e-mail, web browsing or File Transfer Protocol (FTP). However, other applications (e.g., P2P (Peer to Peer) video streaming, online games, etc.) generate high rates of small packets, so the routers may experience problems to manage this traffic, since their processing capacity can become a bottleneck if they have to manage too many packets per second [4]. Finally, in P2P-TV services, the generation of high rates of small packets [5] may penalize the video packets and consequently the peer's behaviour within a P2P structure may not be as expected.

As a consequence of the increase of the amount of small packets generated by emerging services, certain network points may become critical bottlenecks, mainly in access networks. In addition, bottlenecks may also appear at critical points of high-performance networks, being the discarding in router queues the main cause of packet loss. So, the design characteristics of router buffers and the implemented scheduling policies, are of primary importance in order to ensure the correct delivery of the traffic of different applications and services.

Buffers are used as a traffic regulation mechanism in network devices. Mid and low-end routers, which do not implement advanced traffic management mechanisms, are commonly used in access networks. Thus, the buffer size becomes an important design parameter. The buffer can be measured in different ways: maximum number of packets, amount of bytes, or even queueing time limit [6] [7]. Moreover, the buffer must play an important role when planning a network because it can influence the packet loss of different services and applications. Therefore, the QoS of the services can be affected by the size of the buffer and its scheduling policies.

Hence, the characterization of the technical and functional parameters of this device becomes critical when trying to provide certain levels of QoS. This knowledge can be useful for applications and services in order to make correct decisions in the way the traffic is generated. As a consequence, if the size and the behaviour of the buffer are known, some techniques can be used so as to improve link utilization, e.g., multiplexing a number of small packets into a big one, fragmentation, etc. However, a problem appears when using these techniques: device manufacturers do not include all the implementation details in the technical specifications of the devices, but just part of them, mainly those related to the technology used. Thus, if a communication has to cross different networks over the Internet, some knowledge about the device's characteristics

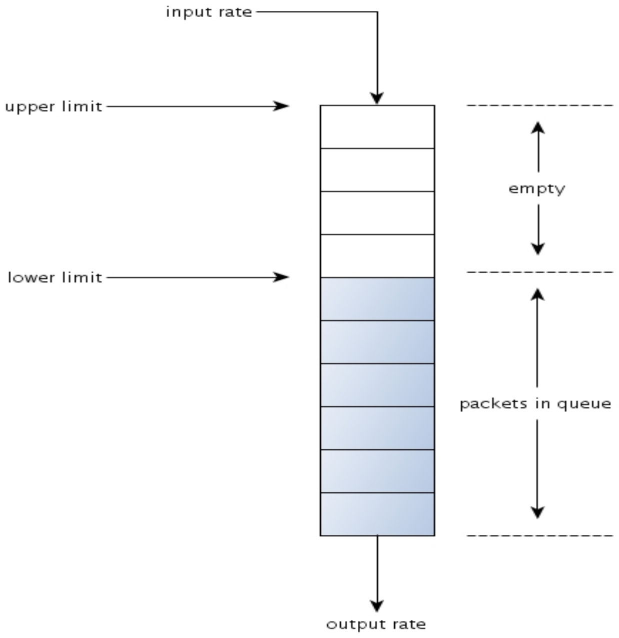


Figure 1. A particular buffer behaviour.

or the buffer's behaviour will be interesting. For these situations, our group is currently working on the development of a tool able to discover some characteristics of the buffer and its behaviour. The final objective is to permit these measurements not only when physical access to the System Under Test (SUT) is granted, but also in the case of only having remote access.

The paper is organized as follows: Section II discusses the related work. The test methodology is presented in Section III. The next section covers the experimental results, and the paper ends with the conclusions.

II. Related Work

A. *Buffer issues*

Buffers are used to reduce packet loss by absorbing transient bursts of traffic when routers cannot forward them at that moment. They are instrumental in keeping output links fully utilized during congestion times.

The so-called *rule of thumb* has been used to obtain the amount of buffering needed at a router's output interface [8] but in [9], a *small buffer* model was proposed, in which buffer size is obtained by the capacity, C, round-trip time, RTT and the number of flows, N, so, $B = C \times RTT/\sqrt{N}$. In [10], it was suggested the use of even smaller buffers, called *tiny buffers*, considering a size of some tens of packets.

Traditional First In First Out (FIFO) queues accept a new packet when there is enough space. However, this is not the only buffer behaviour in commercial devices. In [11], a particular buffer behaviour was observed and characterized: once the buffer gets completely full, no more packets are accepted until a certain amount of memory is available. Thus, an *upper limit* and a *lower limit* can be defined (see Fig. 1): when the *upper limit* is reached, no more packets are accepted until the size of the buffer corresponds to the *lower limit*.

Figure 2. A typical topology in end-to-end communication.

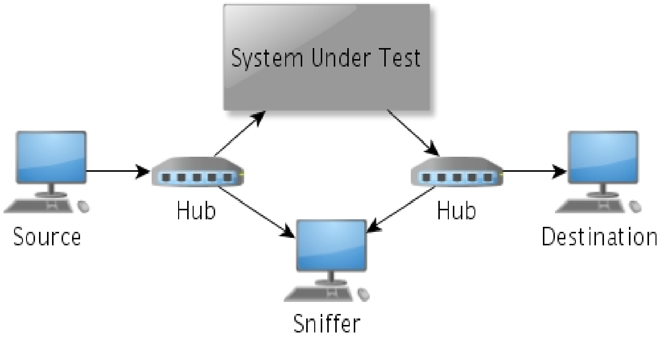


Figure 3. Topology used for tests.

III. Improved Methodology for the Characterization of Internet Paths

When traffic is crossing a network in an end-to-end communication (Fig. 2), all the packets traverse a high number of network devices which may drop packets in some cases. The network path is uncertain for most applications and services which usually only measure the available bandwidth, in order to limit the generated traffic and rarely to smooth it. So, we proposed a method to discover and describe network characteristics which may be useful to correctly modify the traffic by applications. One of the premise of the present work is that most of the network characteristics can be explained by buffers characteristics.

In a previous work [12], we described a methodology to determine the technical and functional characteristics of buffers (as e.g., behaviour, size, limits, input and output rate) of a network path even when more that one buffer is in the path, finding interesting results but with some inaccuracies when obtaining input rate estimations and buffer size. An improvement of this methodology is presented in this article.

A. *Test procedure*

The scheme of the tests is shown in Fig. 3. There is a System Under Test (SUT), which may be either a single device or an entire network. The test is based on the sending of a burst of UDP (User Datagram Protocol) packets from the Source to the Destination machine, so as to produce a buffer overflow in the SUT.

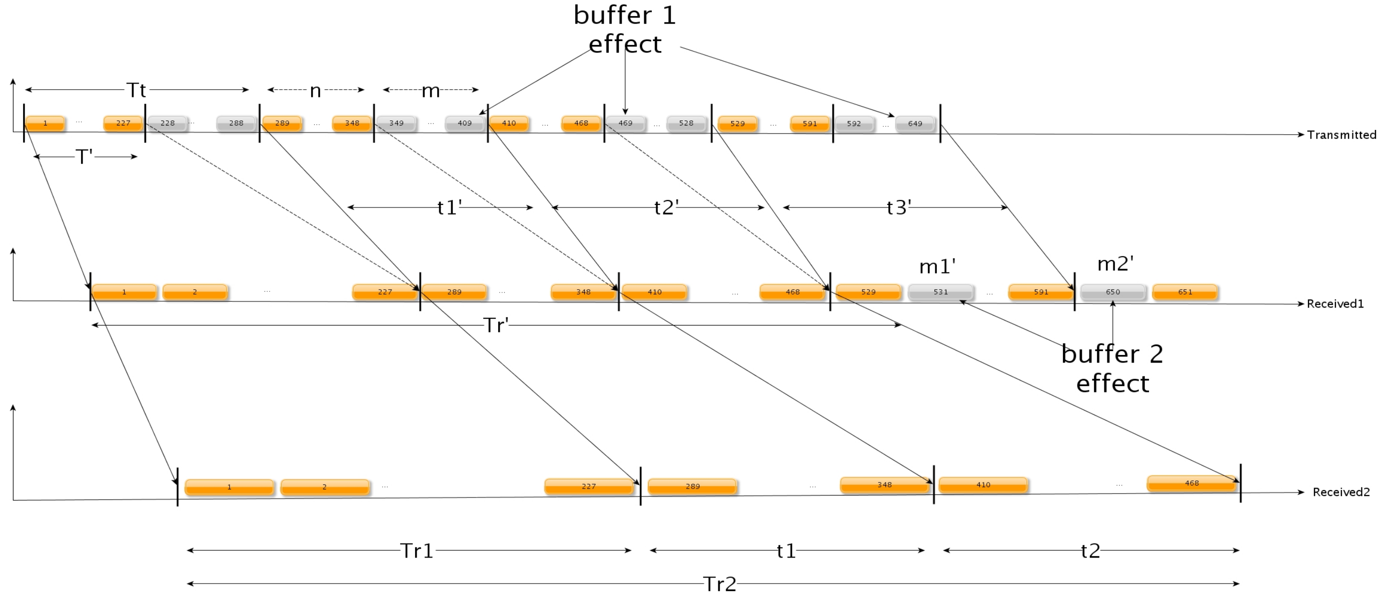


Figure 4. Estimating packets in concatenated queues with remote access.

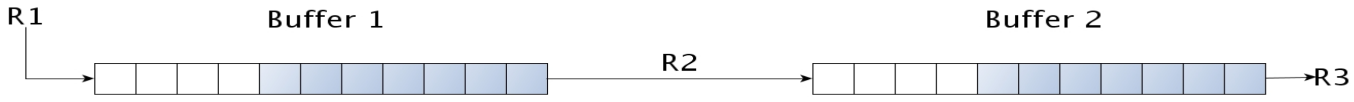


Figure 5. Estimating packets in queue in remote access (particular case).

B. New methodology

The methodology is based on the premise that the output rate can be obtained from traffic capture at the destination device. This output rate depends on the technology used in each case (Ehternet, WiFi). The output rate can be determined because the remote capture includes the n received packets in t seconds, and packet length is known. For calculating the input rate, we know the amount of transmitted packets $n + m$ (received and dropped packets respectively) in t seconds. Where m can be known since all the packets have a unique identifier. With this information, the output and input rates can be estimated only from the data contained in the *destination*.

In Fig. 4, the *Transmitted* trace corresponds to the input of *Buffer* 1; *Received* 1 is the output trace of *Buffer* 1; *Received* 2 is the output trace of *Buffer* 2, and it is the only available trace in order to determinate all the link characteristics. Dropped packets are the grey ones.

Fig. 5 represents an example in which two buffers are concatenated, *Buffer* 1 has an *upper limit* and a *lower limit*, as described in [11]; *Buffer* 2 uses the traditional FIFO policy. These two buffers will fill when $R_1 > R_2 > R_3$. When *Buffer* 1 gets into overflow, it drops packets until a certain amount of memory is available, so it will discard a burst of packets. *Buffer* 2 has a different behaviour in congestion time because if a packet gets out, another one can get into the buffer, so packets will not be discarded in bursts. This figure clearly shown two different packet loss patterns which corresponds to each buffer.

TABLE I. EQUATIONS FOR ESTIMATING BUFFER PARAMETERS OF FIG. 4.

$Rate$	$Buffer\ size$
$R_3 = \frac{n_{rx}}{t_{r2}} \times packet_{size}$	$L_{Buffer1} = \frac{T'_r}{\frac{1}{R_1 - R_2} + \frac{1}{R_2}}$
$R_2 = \frac{n_{rx} + m'_{tx}}{t_n} \times packet_{size}$	$L_{Buffer2} = \frac{T_{r1}}{\frac{1}{R_2 - R_3} + \frac{1}{R_3}}$
$R_1 = \frac{n_{rx} + m_{tx} + m'_{rx}}{t_{r2}} \times packet_{size}$	

Analysing the Fig. 4, we can deduce the rates R and the buffer length L_{Buffer} from the remote capture, we can obtain all the parameters using the expressions shown in Table I, which corresponds to the same variables. In theses equations, the most important parameters are the m values because they correspond to the packet loss pattern of each buffer and they give information about the buffer size. The m values are determined by observing the packet loss patterns and it is given by: $m = number\ of\ patterns$.

We have described the methodology using an example, in which a buffer that drops one packet at a time, is concatenated with other which drops packets in bursts, so the m values or patterns can be easily determined. With the aim of test our methodology, the next section presents a more complex scenario with two concatenated buffers whose packet loss is in burst.

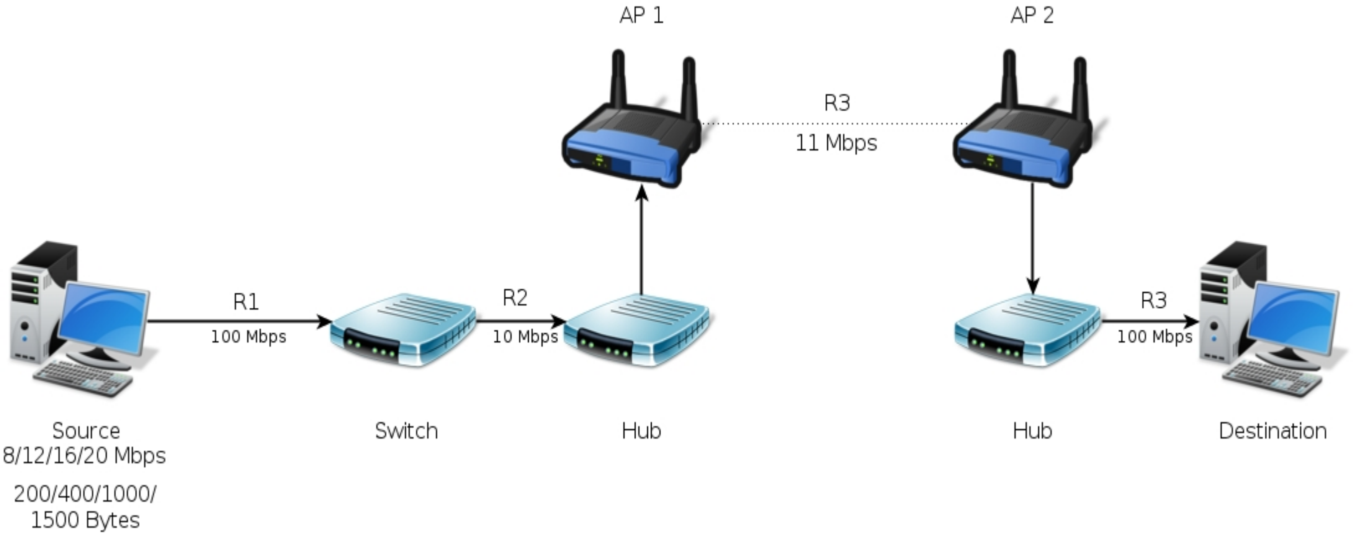


Figure 6. Topology used for estimating the buffer size in wired and wireless network.

IV. Experimental results

Real tests have been deployed in a testbed and results are analysed according to the procedures cited above. Tests have been performed for two different conditions: a single buffer overflow and two different concatenated buffers. The tests are repeated using different values for the packet size and the bandwidth.

A. Laboratory environment

We have implemented a controlled network environment in order to study two different devices: a switch (3COM) and an access point (Linksys WAP54G). The topology is shown in Fig. 6 in which different bandwidth limits were set in the hubs and the access points in order to create a bottleneck to be measured. With the proposed methodology, we will characterize the output buffers of the switch and the access point. Real machines have been used (Linux kernel $2.6.38-7$, $Intel^{\circledR}\ Core^{TM}\ i3\ CPU\ 2.4\ GHz$) for sending and receiving the test packets, in order to identify the buffer behaviour of the devices across the network path.

B. Test procedure

The test is based on the sending of a burst of UDP packets from the source to the destination, so as to produce a buffer overflow on the different devices. The test is intended to find out the bottlenecks that appear, and whether they have the same or different behaviour, according to the size of the sent packets. This test is repeated using different amounts of bandwidth for R_1 $(8, 12, 16, 20\ Mbps)$. The wireless link is set to $11\ Mbps$. Packets of different sizes $(200, 400, 1000, 1500\ bytes)$ are used so as to determine if the buffer is measured in number of packets or in bytes. This information will also be useful to determine the packet size that generates the best results. This allows us to discover when the effect of bottlenecks appears and it will also be useful to determine if the size of the packets may modify the output rate after the bottleneck.

Once the communication is set, we capture the traffic on the end device. This procedure generates a remote capture in the destination host which is analyzed in order to estimate the bandwidth, packet loss and buffer size. The accuracy of these estimations is compared with the one obtained in previous works [11] to validate the method proposed in the present work.

C. Packet loss patron analysis

1) Finding the number of patterns: When the traffic traverses the SUT, packets are lost according to different patterns. If we are able to identify them, this can give us useful information about the number of the buffers in the path. With the aim of finding a number of patterns, we made a study of the packet loss using different amounts of input bandwidth $(8, 12, 16$ and $20\ Mbps)$ which may correspond at the same number of bottlenecks. All the transmitted packets have a length of $1500\ bytes$.

Fig. 7 shows the results for this test. The charts show different packet loss patrons which can be determined by observing the groups of packets around the same packet loss value (see coloured eclipses). The $8Mbps$ graphic, when the input rate is under $10Mbps$ (switch maximum output rate) we can observe that packet loss remains below under 50 packets. There are only a buffer effect, corresponding to the access point WIFI buffer. The $12, 16$ and $20Mbps$ graphic shows that appear three group of packet loss patron. First of them is similar than to the $8Mbps$ graphic, corresponding to the access point WIFI buffer because the output rate of the switch is set to $10\ Mbps$, so the input rate of the access point has no variations. A second group have packet loss close to $125, 160$ and 205 corresponding to the switch buffer. As expected, packet loss increases when input rate grows. But, also, a third group of packet loss is observed and it corresponds to the sum of the packet loss produced by switch and the access point, so this effect is present when both devices drop packets at the same time.

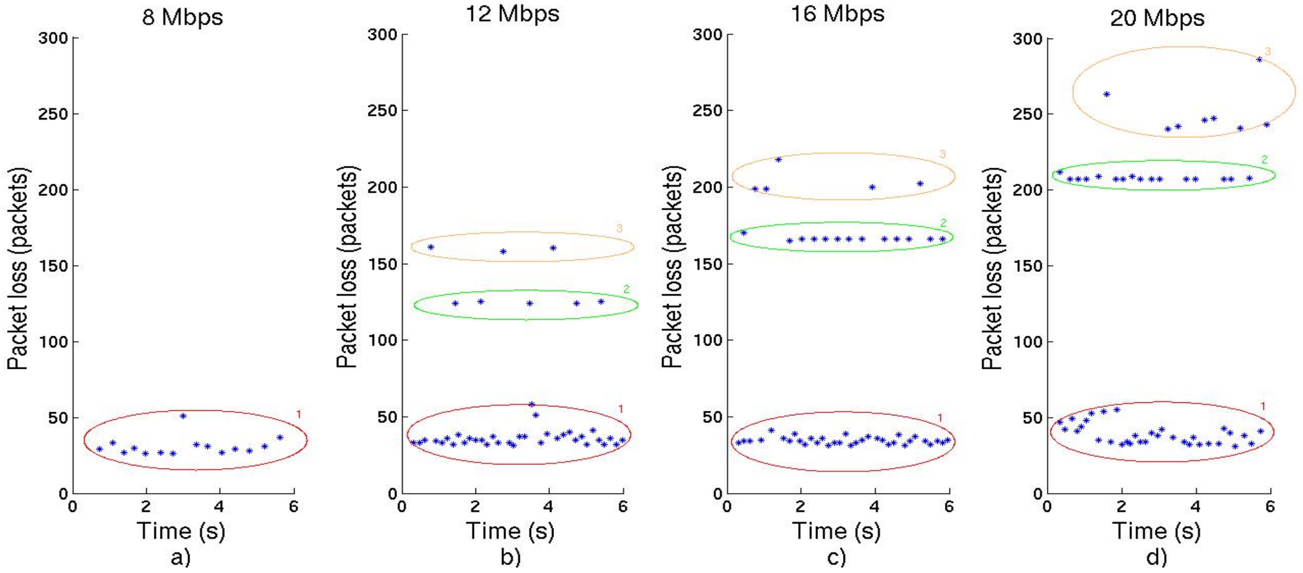


Figure 7. Packet loss patron in the switch and the access point for different bandwidth amounts when packet size is 1500 $bytes$.

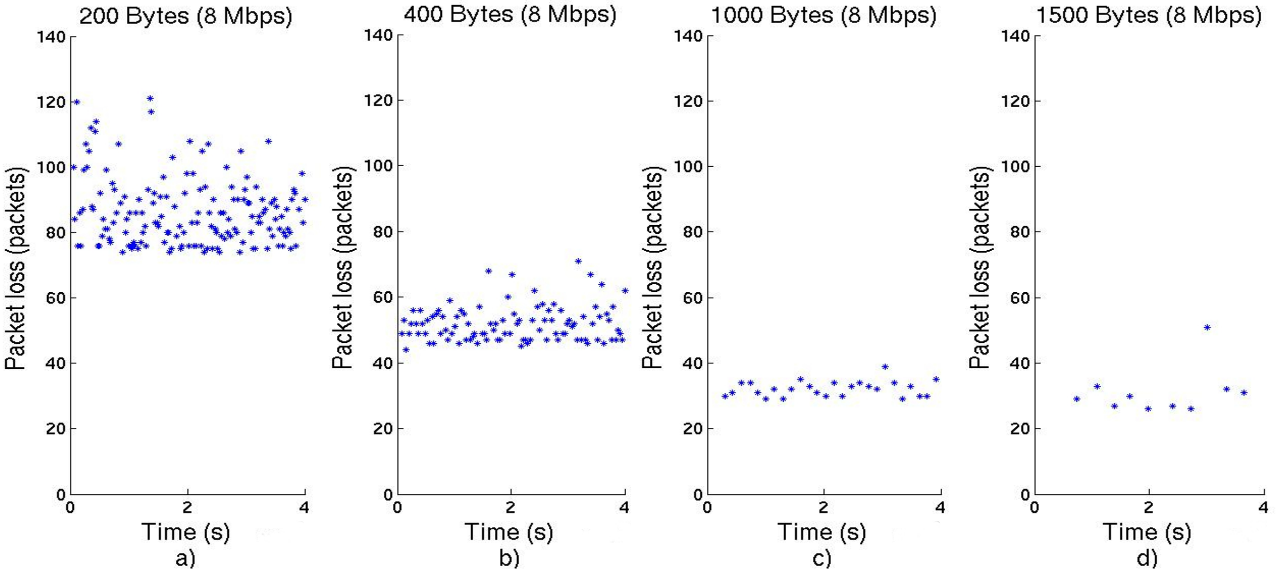


Figure 8. Packet loss patron in the access point for different packet sizes when the bandwidth is 8 $Mbps$.

2) Analyzing the effect of the packet length: In this case we developed two different tests. In the first test, we have selected a bandwidth of 8 $Mbps$ with the aim of producing an overflow on the second buffer ($AP1$) but not on the first one ($Switch$). The test is repeated using packets of $200, 400, 1000$ and 1500 $bytes$. The results are shown in Fig. 8, where different packet loss patterns can be observed.

The amount of lost packets is roughly the same for every test (Fig. 8) and they correspond to the ones obtained in Fig. 7, due to the relationship between the buffer size and the input and output rate of the access point buffer. In the WIFI technology, the output rate increases when packet size increases, so packet loss value is affected by packet length, and it decreases for bigger packets. In addition, packet loss has less dispersion when packet size is bigger.

In the second test (Fig. 9), we used a fixed bandwidth of 20 $Mbps$ in order to flood both buffers. This test allow again us to characterize the relationship between packet size and packet loss pattern. But in this case, the situation is more complex since there are two effects concatenated corresponding to the two buffers. The explanation is similar to the Fig. 7 and 8. There are three groups of packet loss patterns and the different values of the results occurs because the variability of the buffers output rate, which depends on the packets sizes.

3) Estimating the buffer size: We obtained the buffer size for the switch and the access point using to the proposed methodology but analyzing one buffer at a time according to each pattern, and eliminating the effect of the other buffer. In both cases, the appearance of a buffer with *upper limit* and *lower limit* is observed, which maximum size is roughly 120

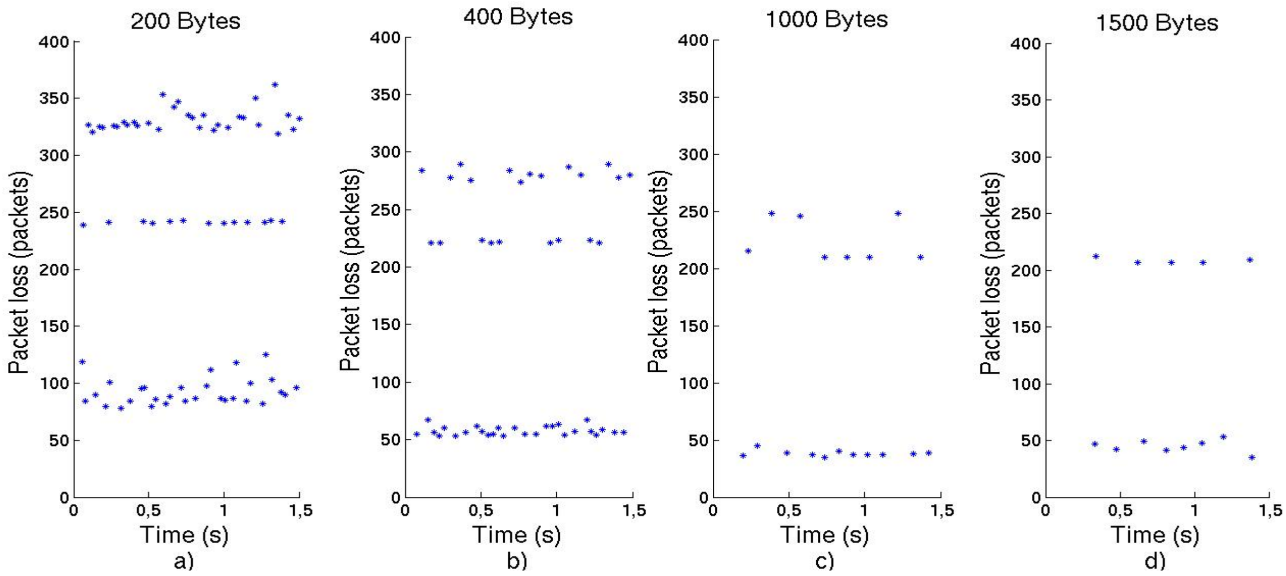


Figure 9. Packet loss patron in the switch and the access point for different packet sizes when the bandwidth is 20 $Mbps$.

packets for the switch and 50 packets for the access point. The more noteworthy is that results are similar that the estimates that we done, in previous works, with isolated buffers.

V. Conclusion

This article has presented a packet loss analysis, which is useful in order to describe the technical and functional characteristics of commercial buffers on a network path. This characterization is important, taking into account that the buffer may modify the traffic characteristics.

Tests using commercial devices have been deployed in a controlled laboratory scenario, including wired and wireless devices. Accurate results of the buffer size and other parameters have been obtained when there is physical access to the "System Under Test". In case of having no direct access to the system, an acceptable estimation can also be obtained.

As future work, the method has to progress in order to improve the accuracy, especially when measuring the input rate when a wireless link is in the network path. Moreover, it would be interesting to discuss how to use the measures to infer on the buffering strategies, which could then lead to transport protocol adjustments that would consider these strategies to maximize QoS.

Acknowledgment

This work has been partially financed by the European Social Fund in collaboration with the Government of Aragón, CPUFLIPI Project (MICINN TIN2010-17298), Ibercaja Obra Social, Project of Cátedra Telefónica, University of Zaragoza, Banco Santander and Fundación Carolina.

References

[1] J. Saldana, J. Fernández-Navajas, J. Ruiz-Mas, J. Murillo, E. V. Navarro, and J. I. Aznar, "Evaluating the influence of multiplexing schemes and buffer implementation on perceived VoIP conversation quality." Computer Networks, vol. 56, no. 7, May, 2012, pp. 1893–1919.

[2] J. Saldana, J. Fernández-Navajas, J. Ruiz-Mas, E. V. Navarro, and L. Casadesus, "The effect of router buffer size on subjective gaming quality estimators based on delay and jitter." in CCNC. IEEE, Jan. 2012, pp. 482–486.

[3] S. Tang, Y. Lu, J. M. Hernndez, F. A. Kuipers, and P. V. Mieghem, "Topology Dynamics in a P2PTV Network." in Networking, ser. Lecture Notes in Computer Science, L. Fratta, H. Schulzrinne, Y. Takahashi, and O. Spaniol, Eds. Springer, May, 2009, pp. 326–337.

[4] W. chang Feng, F. Chang, W. chi Feng, and J. Walpole, "Provisioning on-line games: a traffic analysis of a busy counter-strike server." in Internet Measurement Workshop. ACM, Feb. 2002, pp. 151–156.

[5] B. Fallica, Y. Lu, F. Kuipers, R. Kooij, and P. V. Mieghem, "On the Quality of Experience of SopCast," in Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08. The Second International Conference on, Sept. 2008, pp. 501–506.

[6] A. Vishwanath, V. Sivaraman, and G. N. Rouskas, "Considerations for Sizing Buffers in Optical Packet Switched Networks." in INFOCOM. IEEE, Mar. 2009, pp. 1323–1331.

[7] A. Dhamdhere and C. Dovrolis, "Open issues in router buffer sizing." Computer Communication Review, vol. 36, no. 1, Jul. 2006, pp. 87–92.

[8] C. Villamizar and C. Song, "High performance TCP in ANSNET," SIGCOMM Comput. Commun. Rev., vol. 24, no. 5, Oct. 1994, pp. 45–60.

[9] G. Appenzeller, I. Keslassy, and N. McKeown, "Sizing router buffers." in SIGCOMM, R. Yavatkar, E. W. Zegura, and J. Rexford, Eds. ACM, Feb. 2004, pp. 281–292.

[10] M. Enachescu, Y. Ganjali, A. Goel, N. McKeown, and T. Roughgarden, "Part III: routers with very small buffers." Computer Communication Review, vol. 35, no. 3, Feb. 2005, pp. 83–90.

[11] L. Sequeira, J. Fernandez-Navajas, J. Saldana, and L. Casadesus, "Empirically characterizing the buffer behaviour of real devices," in Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2012 International Symposium on, Jul. 2012, pp. 1–6.

[12] L. Sequeira, J. Fernandez-Navajas, and J. Saldana, "Characterization of the Buffers in Real Internet Paths," in Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2013 International Symposium on, Toronto, Canada, Jul. 2013, pp. 155–160.

Impact of M2M Communications on Cellular Telecommunications Networks

Modeling the effects of M2M Communications on Cellular Core Networks

Bruno de Oliveira Cruz, A. Manuel de Oliveira Duarte
Department of Electronics, Telecommunications and
Informatics, Institute of Telecommunications
University of Aveiro
Aveiro, Portugal
brunocruz@ua.pt, duarte@ua.pt

Ricardo Jorge Moreira Ferreira
PT Inovação
Aveiro, Portugal
ricardo-j-ferreira@ptinovacao.pt

Abstract — **Machine to Machine (M2M) communications have experienced very fast growth in recent times and several forecasts indicate that this trend is going to increase dramatically over the coming years. The traffic generated by M2M services can have very different characteristics as compared to conventional data or voice traffic, heavy burstiness being one its main features. This paper addresses the above issues in the context of cellular networks. Models for signaling and payload throughput in cellular core networks are derived, with particular focus on the effects of aggregated M2M services. These models were implemented in a computational tool that provides visualization of network performance and capacity metrics as function of different service orchestrations. This can be of great usefulness for Mobile Network Operators (MNOs) and other entities that need to understand how to design M2M services and how to deal with their impacts on cellular networks.**

Keywords-Access Networks; Cellular Networks; Core Networks; Internet of Things; M2M; Mobile Networks; Network Planning; Service Orchestration; Traffic Analysis; UMTS.

I. Introduction

Telecommunications services are on the verge of major changes with the rising of Machine to Machine communications and the Internet of Things (IoT). It is expected a growth on the number of connected devices up to 50 billion by 2020 [1]. Such numbers might still be a few years away, but many M2M services are starting to roll out [2].

The effects that M2M related traffic will imply to cellular networks are widely unknown and unstudied, thus it becomes the fundamental objective of this paper to provide models that can be of usefulness to understand such effects, to provide insights on how to design M2M services, and to study the changes that must be enforced on cellular networks.

The focus on cellular networks, is justified by considering that this access technology is the only that can guarantee extremely high rates of coverage. Thus, it is believed that cellular infrastructures are going to be fundamental in the roll-out of services based on M2M technologies.

Additionally, it is expected that traffic generated by many M2M services will present similar characteristics to traffic generated by modern smartphone applications, mainly social networks and instant messaging applications [3]. Thus, this work is believed to be of relevance to services other than M2M.

The traffic generated by M2M services will present very different features when compared to conventional data and voice traffic. Such features will include different patterns of use, with some services presenting high predictability, and others high unpredictability. Many M2M services will generate data transmissions very few times a day, others, a high number of transmissions with very small payloads [4][5]. Burstiness, a statistics concept that refers to the intermittent increases and decreases in the activity or frequency of an event, will also be a typical characteristic for most M2M generated traffic [4][6].

Considering that cellular networks have not been design to deal with this kind of traffic, it becomes urgent to understand how a broad adoption of M2M services will affect the cellular networks. Particularly, considering the number of sessions, the number of subscriptions, and the amount of signaling generated by very small quantities of payload information. Such understanding will provide MNOs with the necessary knowledge to redesign and resize their cellular networks as well as design M2M services, applications, and platforms.

This paper is comprised by eight sections. Section I presents an overview on the problem at study. Section II presents some of the main implications of M2M Communications on Cellular Telecommunications Networks. Section III proposes a model for Universal Mobile Telecommunications System (UMTS) Packet Core (PC) traffic and throughput analysis. Section IV proposes a model for UMTS PC network modeling. Section V proposes a model for service orchestration. Section VI describes a computational tool developed in order to apply the previously referred models. Section VII presents a case study, illustrative of the application of the proposed models, and finally, Section VIII presents the conclusion and discussion, as well as future work on this subject.

II. Impact of M2M Communications into Cellular Networks

Current core network architectures are designed mainly for Human to Human communication, and are not prepared to deal with the foreseeable increase on signaling traffic. Such increase is driven by the growth on M2M and smartphone signaling traffic (growing 50% faster than data traffic [3]). Furthermore, the overall impacts on network capacity and performance, caused by adding a large number of M2M subscriptions to current networks are generally unknown, and may require new levels of scalability, in terms of subscription handling and in terms of mobility and resource management [7]. Considering the explosion of M2M communications, and given that designing a system based on the worst case is very costly [8], it is important to design models and algorithms to depict the networks on large M2M deployment scenarios, allowing for its dimensioning based on average values with some kind of overload control strategies.

Some M2M related factors that might have impact on Core Network performance are:

A. *M2M Traffic Temporal Regime*

M2M communications present a broad number of applications and services. Thus, is no surprise that the M2M traffic temporal regime can be very heterogeneous among different applications and usage scenarios, and consequently its characteristics are diverse and hard to predict. This is a fundamental difference from most Circuit Switched (CS) traffic, adding up to the complexity of analysis of this issue.

B. *Burstiness*

Burstiness is a statistics concept that refers to the intermittent increases and decreases in the activity or frequency of an event, which is characteristic of most of M2M related traffic [4][6]. Understanding the burstiness behavior of data traffic is fundamental, since burstiness introduces sudden peak loads to the network, and is relevant for design and QoS purposes [8]. One of the fundamental design issues related to burstiness is to determine which solution is better: to have devices always in Packet Data Protocol (PDP) active state or to have them constantly activating and deactivating PDP sessions.

C. *Relation between information payloads and signaling overheads*

One of the implications of such decision is on the payload to signaling ratio. Sessions being constantly activated and deactivated will increase dramatically this ratio, with consequences that are not yet known. Some of them might be congestion on elements/functions, such as Authentication, Authorization and Accounting (AAA), Gateway GPRS Support Node (GGSN), Online Charging System (OCS) and Serving GPRS Support Node (SGSN).

D. *Addressability*

On the other hand, if every single device is always with an active PDP session there will be a need for more IP addresses, and probability an expansion on several databases such as Home Location Register (HLR) and Authentication Center (AuC). Such a scenario could require the deployment of IPv6, since IPv4 would not sustain such a network for a long period.

III. Traffic and Throughput Analysis for UMTS Packet Core Networks

The presented work will now focus on UMTS networks, but it can be applicable to other 3GPP technologies. In order to identify the elements and interfaces of the 3G network whose performance and capacity are most critically exposed to negative effects of M2M traffic, a set of models has been developed to calculate payload and signaling throughput on a UMTS network. The following sections present models for Iu-Packet Switched (PS) and Gr interface.

A. *Iu-PS Interface*

The “Iu” interface is comprised of two connections, the Iu-PS interface that interconnects the Radio Network Controller (RNC) and the SGSN and the Iu-CS interface that connects the RNC to the Media Gateway (MGW). The MGW is part of the CS domain and therefore the Iu-CS interface will not be considered in the following calculations (M2M communications will be supported by the Packet Core). Adapting the work presented in [8][9], the following equations can be formulate:

1) *The overhead ratio in Iu-PS interface is given by:*

$$RO_{Iu-PS} = \frac{S_{Packet} + H_{IuUP} + H_{GTP} + H_{UDP} + H_{IP} + H_{MPLS}}{S_{Packet}}. \quad (1)$$

where:

- “S_{Packet}” is the average IP packet size [bytes];
- “H_x” is the header size of “x” packet, as depicted on Table I [bytes].

TABLE I. Protocol stack of Iu-PS Interface - Based on [8][9]

Radio Network Control Plane		PS Data Plane	Header Size	OSI model
RANAP		Iu-UP	HIu-UP	layer 4, Transport
SCCP				
MTP3-B	SCTP	GTP-U	HGTP	
SSCF-INI	IP	UDP / TCP	HUDP	
SSCOP		IP	HIP	3, Network
MPLS		MPLS	HMPLS	2, Data Link
layer 1, Physical				

2) *The throughput of data plane in the Iu-PS interface (expressed in bps) is given by:*

$$TH_{UP_{IuPS}} = N_N * R_{Attach} * R_{\frac{Active}{Attach}} * Th_{Node} * RO_{Iu-PS} * f_d. \quad (2)$$

where:

- “N_N”, “R_{Attach}”, “$R_{\frac{Active}{Attach}}$”, and “$Th_{Node}$” are defined on Table IV;
- “RO_{Iu-PS}” is the overhead ratio in Iu-PS interface, given by (1);
- “f_d” is the data throughput redundancy factor.

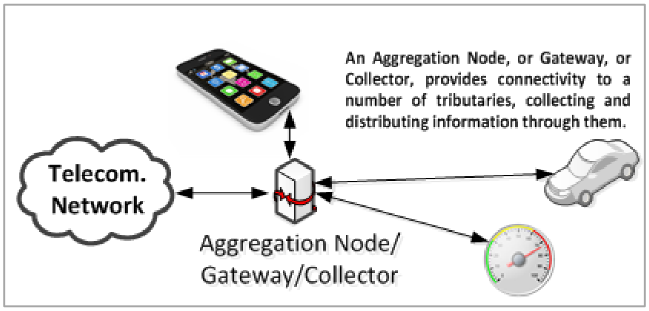

An Aggregation Node, or Gateway, or Collector, provides connectivity to a number of tributaries, collecting and distributing information through them.
Telecom. Network
Aggregation Node/ Gateway/Collector

Figure 1. Aggregation Node (AN) definition.

Table II lists eleven basic types of messages that can be estimated by MNOs and that comprise most of the throughput in control plane of Iu-PS interface.

TABLE II. FOOTNOTES FOR (3) - BASED ON [8][9]

i	N_{IuPS_i}	L_{IuPS_i} [bits]	Relevant for M2M comm.
1	Authentication times per hour	Length of messages per authentication	yes
2	Attachment times per hour	Length of messages per attachment	
3	Detachment times per hour	Length of messages per detachment	
4	Inter SGSN route update times per hour	Length of messages per inter SGSN route update	only if M2M service requires mobility
5	Intra SGSN route update times per hour	Length of messages per intra SGSN route update	
6	Intra SGSN Serving Radio Network Subsystem (SRNC) route update times per hour	Length of messages per intra SGSN SRNC	
7	PDP activation times per hour	Length of messages per PDP activation	yes
8	PDP deactivation times per hour	Length of messages per PDP deactivation	
9	Periodic SGSN route area update times per hour	Length of messages per periodical SGSN route update	
10	SMS mobile originated times per hour	Length of messages per SMS service	only if M2M service requires SMS
11	SMS mobile terminated times per hour		

3) Thus, the signaling load of Iu-PS interface (expressed in bps) is given by:

$$S_{IuPS} = N_N * R_{Attach} * \sum_{i=1}^{11}\left(N_{IuPS_i} * L_{IuPS_i}\right) * \frac{1}{3600} * f_s. \qquad (3)$$

where:

- "N_{IuPSi}" is given by Table II;
- "L_{IuPSi}" is given by Table II;
- $\frac{1}{3600}$ is used to convert hours to seconds;
- "f_s" is the signaling throughput redundancy factor.

Table II messages comprise the signaling of Iu-PS interface. Messages such as P-Temporary Mobile Subscriber Identity re-allocation message, identification check message, and service request message are not considered in (3) due to their small size and reduced usage. If proven necessary to integrate them into the Equation, a redundancy factor can be imposed (f_s). The number of periodic Route Area Updates (RAUs) is determined by:

$$N_{Route_{periodic}} = \frac{N_N\ (1-R_{Active})}{P_{Refresh}*3600}. \qquad (4)$$

where:

- "$P_{Refresh}$" is the periodic RAU interval [s];
- 3600 is used to convert seconds to hours;
- "$N_N\ (1 - R_{Active})$" is the number of idle ANs.

B. Gr interface

Applying the same method is possible to define the signaling load going through Gr interface (expressed in bps):

$$S_{Gr} = N_N * R_{Attach} * \sum_{i=1}^{3}\left(R_{Gr_i} * N_{Gr_i} * L_{Gr_i}\right) * \frac{1}{3600} * f_s. (5)$$

where:

- "R_{Gri}" is given by Table III;
- "N_{Gri}" is given by Table III;
- "L_{Gri}" is given by Table III.

TABLE III. FOOTNOTES FOR (5) - BASED ON [8][9]

i	R_{Gr_i}	N_{Gr_i}	L_{Gr_i} [bits]	Relevant for M2M
1	Authentication Rate	Authentication times per hour	Length of messages per authentication	yes
2	Attach Rate	Attach times per hour	Length of messages per attachment	
3	not applicable	Inter SGSN route update times per hour	Length of messages per inter SGSN route update	only if requires mobility

The same methodology can be applied to other UMTS PC interfaces.

IV. UMTS PACKET CORE NETWORK MODELING

Using the throughput models from the previous section it is possible to design a mathematical model of the throughputs and capacity of an UMTS PC Network.

In order to study such network, let us consider the model presented on Figure 2, where:

- "w_i" is the raw throughput capacity for interface "i" [bps];
- "SIG_{i_x}" is the signaling capacity for interface "i" of Network Element (NE) "x" [bps];
- "w_{i_x}" is the raw throughput capacity for interface "i" of NE/System "x" [bps].

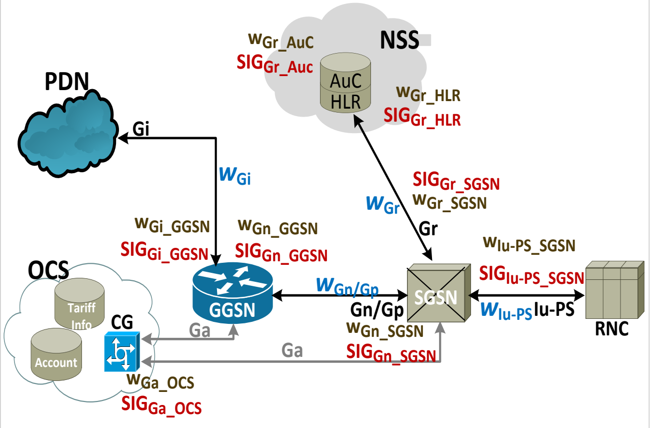


Figure 2. Mathematical description for the UMTS Packet Core Network model.

This model is useful in order to develop a computational tool capable of applying the models proposed in Section III.

V. SERVICE ORCHESTRATION

The traffic models presented in previous sections require knowledge about the aggregated M2M traffic coming from the user side. This section presents an orchestration model capable of providing an approximation for this aggregated traffic as function of different usage profiles.

Table IV presents the variables that must be defined for each service to consider on the orchestration operation.

TABLE IV. PARAMETERS FOR SERVICE ORCHESTRATION

Variable	Symbol	Description
Number of connections	N_N	Number of subscriber devices (Smartphones, ANs, Cars, etc).
Throughput	Th_{Node}	Node throughput (aggregated throughput of several tributaries) [bps].
Sessions / Hour	N_{IuPS_7}, N_{IuPS_8}, N_{Gni}	Number of service sessions per hour; Correspondent to the number of PDP activation / deactivation requests.
Attachments / Hour	N_{IuPS_2}, N_{IuPS_3}, N_{Gr_2}	Number of attachment times per hour; Considered to be correspondent to the number of detachment times per hour.
Authentications / Hour	N_{IuPS_1}, N_{Gr_1}	Number of authentication operations per hour.
Intra SGSN route updates / Hour	N_{IuPS_5}, N_{IuPS_6}	Number of Intra SGSN and Intra SGSN SRNC route update times per hour.
Inter SGSN route updates / Hour	N_{IuPS_4}, N_{Gr_3}	Number of Inter SGSN route update times per hour.
Periodic SGSN RAUs / Hour	N_{IuPS_9}	Number of periodic SGSN RAU times per hour.
Authentication Rate	R_{Gr_1}, $R_{auth_{HLR}}$	Ratio of authentication that needs to get parameters from HLR [%].
SMSs MO / Hour	$N_{IuPS_{10}}$	Number of SMSs Mobile Originated per hour.
SMSs MT / Hour	$N_{IuPS_{11}}$	Number of SMSs Mobile Terminated per hour.
Premium Subscr. Ratio		Ratio of premium subscribers. [%].
Regular Subscr. Ratio		Ratio of regular subscribers [%].
Basic Subscr. Ratio		Ratio of basic subscribers [%].
Attached Subscribers Ratio	R_{Gr_2}, R_{Attach}	Ratio of attached subscribers [%].
Active/Attached Subscribers Ratio	$R_{\frac{Active}{Attach}}$	Ratio of attached subscribers with active session [%].

The node throughput is given by the sum of the several tributaries/services throughputs:

$$T_{node} = \sum Th_k. \tag{6}$$

where:

$$Th_k = \frac{\delta}{t_\delta + t_t}. \tag{7}$$

$$t_t = N_{Packets} * t_{bP}. \tag{8}$$

$$N_{Packets} = \frac{\delta}{P_{size}}. \tag{9}$$

where:

- "Th_k" is the throughput generated by the service "k" [bps];
- "δ" is the average size of the data message to be transmitted [bits];
- "t_δ" is the time between data messages transmissions [s] (see Figure 3);
- "t_t" is the time of transfer [s] (see Figure 3);
- "$N_{Packets}$" is the number of packets needed to transfer the required data;
- "t_{bP}" is the mean time between Packets within a Packet burst [s] (see Figure 3);
- "P_{size}" is the average packet size [bits].

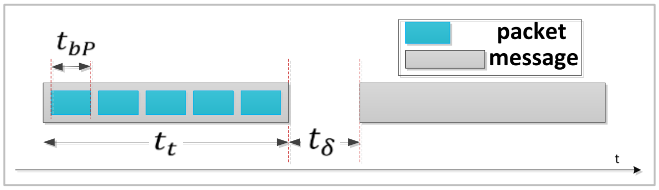


Figure 3. Equation (7) and (8) time relationships.

ISBN: 978-1-61208-324-7

Equations (7) to (9) are adapted from [10].

VI. Computational Tool

In order to provide a visualization and interactive environment based on the previously presented models, a computational tool has been developed with the objective of calculating and providing visual representations of network behavior as a function of different service orchestrations. The tool flowchart is depicted on Figure 4.

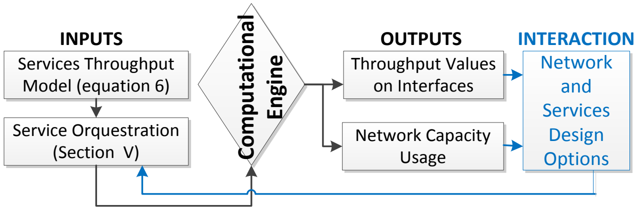

INPUTS
Services Throughput Model (equation 6)
Service Orquestration (Section V)
Computational Engine
OUTPUTS
Throughput Values on Interfaces
Network Capacity Usage
INTERACTION
Network and Services Design Options

Figure 4. Computational tool flowchart.

Although this paper studies UMTS, this tool can be applicable to other 3GPP technologies.

VII. Case Study

A. Example of Application

To illustrate the applicability of proposed models, let us consider a case study where it will be studied the uplink capacity usage of Iu-PS and Gr interfaces as a function of M2M services usability. Let us consider a UMTS network with the following characteristics:

- $w_{Iu-PS} = w_{Iu-PS_{SGSN}}$ = 100.000 Mbps;
- $w_{Gr} = w_{Gr_{SGSN}}$ = 500 kbps.

The service orchestration is based on the following elements:

- Baseline service set (CS and PS services already present in the network before the introduction of M2M services);
- M2M service set (e.g., Smart Metering, Home Automation, Healthcare, Security, etc.).

In order to calculate the capacity usage prior to considering M2M services, i.e. the baseline service set, the model described in equations (6) to (9) will be applied to the various services under consideration (PS services such as browsing, email, social networks, streaming, etc., and PS services such as voice calls and Short Message Service (SMS)). As an example of the method applied, calculations for email are presented on Table V.

Let us now consider that replicating these calculations for other services, and considering that 100,000 cellular subscribers (assumed to be, mainly, smartphone subscribers) are being served, the values for Iu-PS and Gr baseline usage (uplink) can be calculated [11] and will provide the following values:

- Iu-PS usage baseline: 105 Mbps (of which, 3% is signaling);
- Gr usage baseline: 350 kbps (of which, 100% is signaling).

TABLE V. Email Profiling

	Downlink	Uplink
Average size of message (δ)	75,00 Kbytes	20,00 Kbytes
Average Packet size (P_{size})	800 bytes	800 bytes
Number of Packets ($N_{Packets}$)	93,75	25,00
Mean time between Packets within burst (t_{bP})	0,015 s	0,015 s
Time between data message transmissions (t_{δ})	1200 s	1200 s
Time of transfer (t_t)	1,41 s	0,38 s
Email throughput (Th_{email})	0,50 kbps	0,27 kbps

TABLE VI. M2M Service Orchestration

M2M service	Smart Metering	Healthcare	Automotive	Public Transportation	Security
N_N	50.000	50.000	50.00 0	1.000	10.000
Th_{Node} [kbps]	0,50	1,00	0,50	0,50	1,00
S_{packet} [bytes]	130	130	130	130	130
N_{Attach}	2,00	13,42	0,42	60,00	8,00
N_{Detach}	2,00	13,42	0,42	60,00	8,00
$N_{PDP_{activation}}$	2,00	13,42	0,42	60,00	8,00
$N_{PDP_{deactivation}}$	2,00	13,42	0,42	60,00	8,00
$N_{SRNC_{intra-SGSN}}$	0,00	0,03	0,07	1,00	0,10
$N_{SRNC_{inter-SGSN}}$	0,00	0,01	0,03	0,01	0,01
$R_{auth_{HLR}}$	20%	20%	20%	20%	20%
$N_{SMS_{MO}}$	0,00	0,00	0,00	0,00	0,00
$N_{SMS_{MT}}$	0,10	1,00	0,80	0,00	0,00
$R_{\frac{Up}{Total}}$	100%	100%	100%	100%	100%
$f_{redundancy_{data}}$	1,10	1,10	1,10	1,10	1,10
$f_{redundancy_{signaling}}$	1,00	1,00	1,00	1,00	1,00
R_{Attach} , $R_{\frac{Active}{Attach}}$	Please refer to Figure 5				

For sake of simplicity, it shall be considered that the baseline usage is constant through the 24 hours of the day.

The network at study will provide connectivity for a set of M2M services, which are considered to be as presented on Table VI and Figure 5.

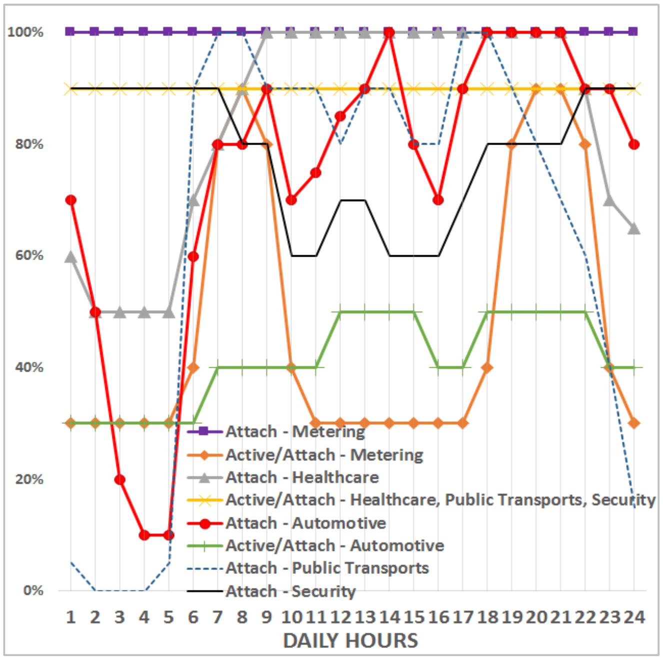


Figure 5. 24 Hourly usage profile for M2M services.

In order to apply the proposed models, the header size for the protocol stack of the interface Iu-PS must be known.

Assuming that header values for the Iu-PS interface are as presented on Table VII, and applying them to (1), it comes:

$$RO_{Iu-PS} = 1{,}40.$$

TABLE VII. HEADER SIZE FOR IU-PS INTERFACE - BASED ON [9]

User Plane	Header Size [bytes]
Iu-UP	4
GTP-U	12
UDP	8
IP	20
MPLS	8
Total	**52**

In order to apply (3) and (5), it is necessary to know the length of messages, which are considered to be as presented on [9].

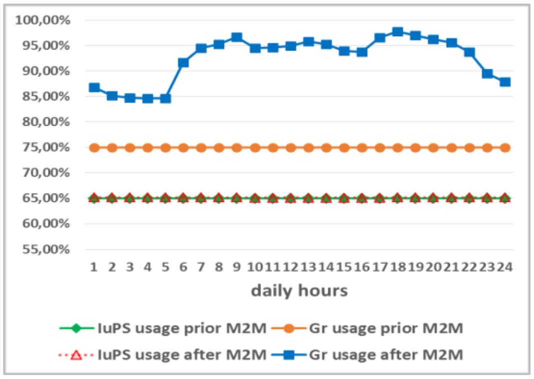


Figure 6. Case study results.

Now that every variable has been presented, it is possible to input the service orchestration parameters of Table VI into the computational tool, and visualize results. For this case study, the tool provides the results of Figure 6, which shows uplink usage rates (%) for the Iu-PS and Gr, prior and after the addition of M2M services.

By analyzing this figure, it can be concluded that the impact of M2M traffic on Iu-PS interface is negligible, since the payload generated by these M2M services is small, and the amount of signaling is small relatively to the capacity of this interface. However, on Gr interface it is visible a considerable increase on capacity usage, showing that M2M services have increased significantly the amount of control information being carried by this interface (HLR, AuC). In the scenario at study, after considering M2M services, Gr interface is dangerously close to its full capacity, which could originate network congestion and QoS/QoE degradation.

B. *Sensitivity Analysis for Orchestration Parameters*

An important feature provided by the developed tool is that it allows service developers to foresee how the network will respond as a function of service orchestration and parameterization scenarios. In order to identify which service parameters could be problematic to the network performance, a sensitivity analysis for the M2M service orchestration parameters is presented as a function of different interface usage ratios when varying a set of service orchestration parameters. To this purpose, the tool was configured to consider a M2M service, characterized by the following parameter values (typical of a smart-metering service):

- 8.500 Aggregation Nodes;
- Transmission Interval: 30 minutes;
- Ratio of authentication that needs to get parameters from HLR ($R_{auth_{HLR}}$): 20%;
- Average Packet size (P_{size}): 130 bytes;
- Gr uplink capacity (w_{Gr}): 1 Mbps;
- Other interfaces uplink capacity: 10Mbps.

The parameters that were considered in this sensitivity analysis were the transmission interval, the ratio of authentication that needs to get parameters from HLR, the average Packet size and the number of SMSs per hour.

The results of this analysis are presented on Figure 7, from where it can be observed that the transmission interval will be the most influential constraint for the considered M2M services. For small values of transmission interval, the impact of M2M overheads can vary noticeably, particularly in Gr and Iu-PS. Concerning the other parameters at study, no major design constraints are expected, except for services that will require a considerably large amount of SMSs.

VIII. Conclusion and Future Work

This paper presented mathematical models that can be useful to better understand the effects of M2M related traffic into cellular telecommunications networks. As a result of this work a prototype for a computational tool was developed, that is believed to be of value to MNOs and future research in this field. The results presented, although mainly illustrative, support the usefulness of this models and tool. The presented work needs further developments and improvements, mainly in the orchestration of usage scenarios, which implies an extended development of the proposed models and a deeper knowledge on the characteristics of M2M traffic sources, accordingly to different types of services and usage scenarios. Although influenciated by previous work [8][9], the models presented on Section III represent a novel insight to study the UMTS Packet Core. Their application to the study of M2M communications is, to the best knowledge of the authors, a new application to such model. The resultant computational tool has already proven to be of practical benefit to real world application.

Acknowledgment

The work reported in this paper has been supported by Portugal Telecom through PT Inovação. This support is deeply appreciated. The Financial contribution of Portuguese National Science Foundation (FCT) is also deeply appreciated.

References

[1] M. Alendal, “Operators need an ecosystem to support 50 billion connections”, Ericsson Business Review, no. 3, 2010, p. 42.

[2] Electronic Publication: “The M2M adoption barometer 2013”, Vodafone Group, 2013.

[3] Electronic Publication: “Signaling is growing 50% faster than data traffic”, Nokia Siemens Networks, 2012.

[4] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, “A First Look at Cellular Machine-to-Machine Traffic Large Scale Measurement and Characterization”, Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, USA, AT&T Labs – Research, Florham Park, NJ, USA, 2012.

[5] A. Orrevad, “M2M Traffic Characteristics”, KTH Royal Institute of Technology, Stockholm, Sweden, 2009.

[6] S. Resnick, “Data Network Models of Burstiness”, School of Operations Research and Industrial Engineering - Rhodes Hall, Cornell University, Ithaca NY, USA, Aug, 3, 2005.

[7] M. Corici, J. Fiedler, T. Magedanz, and D. Vingarzan, “Evolution of the Resource Reservation Mechanisms for Machine Type Communication Over Mobile Broadband Evolved Packet Core Architecture”, Fraunhofer FOKUS Institute, Berlin, 2011.

[8] M. C. Chuah and Q. Zhang, Design and Performance of 3G Wireless Networks and Wireless LANs, New York, NY: Spinger, 2006, pp. 3–223.

[9] Y. Ouyang and M. H. Fallah, “An Analysis of Traffic and Throughput for UMTS Packet Core Networks”, International Journal of Interdisciplinary Telecommunications and Networking (IJITN), vol. 2, issue 2, pp. 1–26, 2010.

[10] Personal Communication between A. M. de Oliveira Duarte, University of Aveiro, and B.R Jarmo, NOKIA, May 22, 2001.

[11] B. de Oliveira Cruz, A. Manuel de Oliveira Duarte, and R. J. Moreira Ferreira “Impact of M2M Communications on Cellular Telecommunications Networks”, Internal Report, University of Aveiro, 2014.

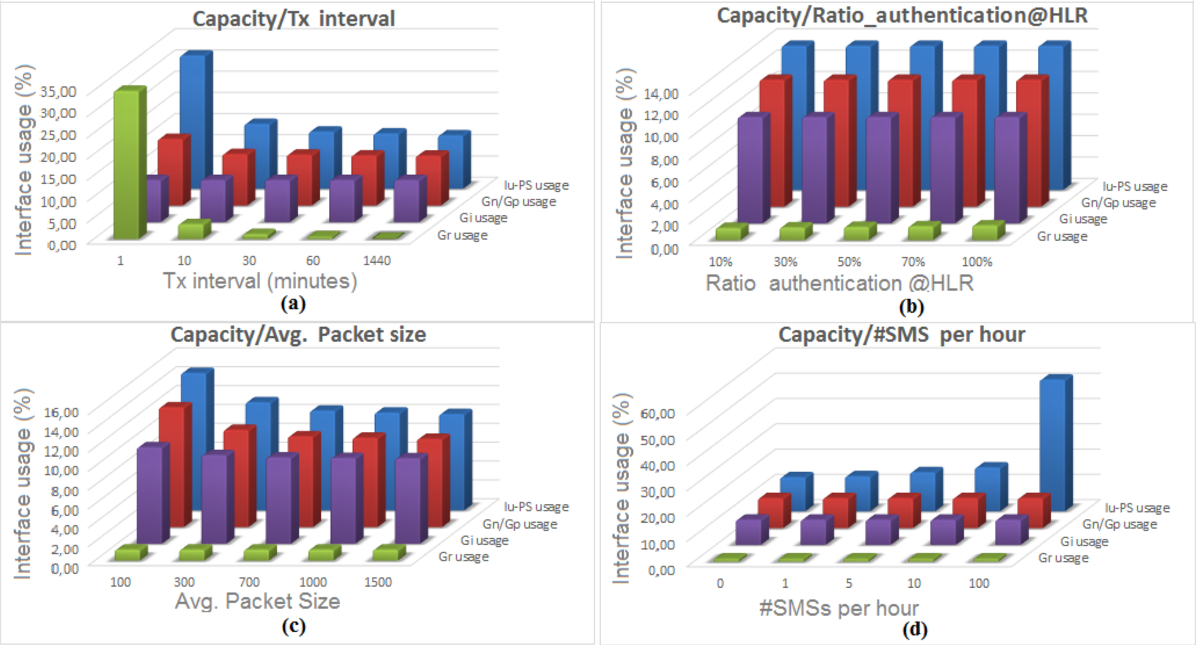


Figure 7. Sensibility analysis results: (a) Varying .the transmission interval; (b) Varying the ratio of authentication that needs to obtain parameters from the HLR; (c) Varying the average Packet size; (d) Varying the number of SMSs per hour

Trust Blueprints and Use Cases

Deepak Vij, Ishita Majumdar, Naveen Dhar
FutureWei Technologies, Inc.
US Central Research Institute
Santa Clara, California, USA
e-mail: {Deepak.vij, Ishita.majumdar,
Naveen.dhar}@huawei.com

George Vanecek, Jr.
FICO
Product and Technology Organization
San Jose, California, USA
e-mail: {georgeVanecek}@fico.com

***Abstract*—As the scope of current distributed computing model envisioned by the contemporary cloud computing environment enlarges to future federated *Intercloud* and ubiquitous and pervasive computing models such as *Internet of Things* (IoT), many difficult problems and challenges arise. Security is one of the most important concerns of such a computing environment. Current security mechanisms are very static, inflexible and not granular enough to make efficient and informed decisions in the *Service Provider* based computing environment. The conventional trust mechanisms in place are inadequate at addressing granular level trust issues in the highly distributed open environments. In this paper, we explore various Trust Management schemes and blueprints for enabling a framework that interested parties can use to determine the trustworthiness of disparate and heterogeneous computing entities. The paper also enumerates various business use case scenarios articulating how such a *Trust Management* framework would be invaluable for addressing the current as well as future computing environments needs.**

Keywords-Trust Management; Internet of Things; Cloud Computing; Device Mobility; Authentication; XACML; Authorization; Intercloud; Context-Awareness; Evidence-based Trust.

I. INTRODUCTION

In recent years, the contemporary highly distributed and heterogeneous cloud computing design pattern has ushered in an era of tremendous breakthroughs in geographical distribution, resource utilization efficiencies, and infrastructure automations. Yet, as the scope of current distributed computing model envisioned by the contemporary cloud computing environment enlarges to future federated *Intercloud* and ubiquitous and pervasive computing models such as *Internet of Things* (IoT), many difficult problems and challenges arise. Security is one of the most important concerns of such a computing environment. Current security mechanisms are very static, inflexible and not granular enough to make efficient and informed decisions in the *Service Provider* based computing environment. The conventional trust mechanisms in place are inadequate at addressing granular level trust issues in the highly distributed open environments.

Typically, security architecture facilitates the trust mechanisms between two entities whereby the *truster* is an entity that trusts another entity, the trustee, and the *trustee* is an entity that is being trusted. Traditional security architecture is built around regulating access to target resources or services by granting certain *authorization* rights to *authenticated* entities (*trustee*). Authentication and authorization processes work in tandem as part of the overall access management architecture.

Authentication is the process through which an entity (e.g., a person, device or service) provides sufficient credentials such as passwords, tokens, public key certificates (using public-key infrastructure - PKI) or secret keys to satisfy access requirements of a resource, based on a pre-existing membership of that entity. Authentication is essentially a process of ensuring irrefutable knowledge of the trustee (entity). It enables users, computers or devices to know with whom they are communicating.

Authorization, on the other hand, is the process used to determine *what* services or resources an irrefutably known authenticated user, computer or a device, can access. Authorization is a process for protecting resources and information while allowing seamless access for legitimate use of those resources. It allows security administrators to enact authorization entitlement policies in an easy to maintain and simple to monitor fashion.

Traditionally, authentication services helped a computer identify a person attempting to gain access, or to *log on*. In the last decade or so, authentication needs have evolved to go beyond the traditional scope of simple *log on* process. These new authentication schemes include PKI based *digital signatures* technique. Cryptographic algorithms-based digital signatures, as the name implies, mark an electronic document (digital certificate) to signify its association with an entity. A trusted third party that certifies the digital signature issues the digital certificate.

Irrespective of the authentication mechanism, a successful authentication process assigns a static/fixed *role* to the *trustee* (or *requester*). The authorization process, in turn, determines the access control based on the fixed role assignment. It is important to note that access control to resources is not assigned directly to the *requester* entities but to abstractions known as *roles*. As *entities* are assigned to different roles, they indirectly receive the relevant access control privileges.

With the distributed computing and cloud models moving towards a federated *Intercloud* model [1][2][3] along with the near ubiquity and pervasiveness of smart devices and sensors (*Internet of Things*), these classic authentication and authorization methods pose challenges. With the humanization of Internet technologies whereby smart devices are increasingly taking on more intelligent and autonomous roles for their owners, it is equally important for services to obtain real-time and context-specific information about trustworthiness of its users.

Effective provisioning and delivery of application services in an efficient and more importantly, in a highly secured manner, are the key challenges faced going forward. It has become increasingly important to be able to generate dynamic, granular security policies for federated ubiquitous systems.

Current security techniques that are widely being employed include sand-boxing, PKI based cryptography, and other access control and authentication mechanisms. These mechanisms, however, are very static, inflexible and not granular enough in order to make efficient and informed decisions for the future computing environment.

Specifically, explicit *trust* [4][5][6], for the most part, is conspicuously left out of the contemporary fabric of the Internet. Contemporary rudimentary *trust* mechanism applies to individuals only and is not made integral part of the fabric of the Internet and the Web itself. Current conventional trust mechanisms are inadequate at addressing granular level and real-time, contextual trust issues in the highly decentralized open environments.

Trust needs to be established from the viewpoint of both parties (*Service Requesters* and *Service Providers*). *Service Requester's* trust with respect to the *Service Provider* may be different from *Service Provider's* trust with respect to the requester. From *Service Requester's* perspective, trust towards the *Service Provider* signifies correct and faithful allocation of resources as part of the efficient execution environment with respect to established trust and other security policies. From *Service Provider's* perspective, trust towards *Service Requester* will generate a legitimate request consisting of virus free code and will not produce malicious results and does not temper other results/information/code present at *Service Provider's* end.

With this as the backdrop, this paper proposes detail blueprints of a *Trust Management* system describing the key components within the proposed system and how these components interact with each other. The paper explores various *Trust Management* schemes and blueprints for enabling a framework so that interested parties can determine the trustworthiness of disparate and heterogeneous computing entities. The paper also enumerates various business use case scenarios articulating how such a *Trust Management* framework would be invaluable for addressing the current as well as future computing environment needs.

This paper describes various components of the *Trust Management* system in detail and strives to provide a general foundation for building various constituents of the trust system. However, the paper does not delve deep as far as describing the actual mathematical algorithms/functions and in-depth technology details for underlying components. Our future work will publish such in-depth details for each and every components of the *Trust Management* system.

We will attempt to demonstrate our proposed Trust Management system's paradigm shift in comparison to the typical role-based access control computer security model. In the future, with open and highly decentralized environment where entities are dynamic in nature, the identity of every entity is not known in advance. In such an environment, traditional fixed *role* assignment becomes an irrational and ad-hoc exercise and not viable at all. Although, PKI based credentials mechanism implement a notion of trust, this trust is static and binary in nature. Access privileges are allowed or credentials are rejected and the *trustee* entity does not get the access rights. In such a highly de-centralized environment, the static role assignment needs to be evolved in such a manner that it enables a dynamic trust value assigned to a *trustee* entity. Trust based authorization mechanism, in turn, leverages the dynamic trust value assigned to the *trustee* entity and makes the access control decisions accordingly in a highly dynamic manner.

The rest of the paper is organized as follows: Section II outlines a brief description of *Trust based Paradigm Shift* as well as formal definitions related to *Trust Paradigm*. Section III outlines the proposed overall *Trust Management* system blueprints. Section IV enumerates various business use cases. Finally, Section V presents our conclusions.

II. TRUST BASED PARADIGM SHIFT – AN OVERVIEW

Trust reflects the expectation one actor has about another's future behavior to perform expected activities dependably, securely, and reliably based on experience collected from previous interactions and relevant external sources. Our definition of *Trust* is based on a paradigm shift assumption that formalizes trust so that trust considerations may be added to how future services and computer systems communicate amongst each other.

The key tenet of our proposed trust model is that the *truster* decides permissions based on Principle's set of attributes instead of principle's identities. Trust attributes may include *Evidence-based* as well as *Reputation-based* attributes whereby entities endow other unknown entities in order to gain access to services or resources in a highly federated distributed environment. Traditional mechanisms, on the other hand, are typically based on the key assumption that identity of every entity is known in advance.

This section explains the overall trust based paradigm that includes, trust properties, trust entities, trust contexts and situations and belief policies and intent.

A. Trust Properties

We define trust as possessing the following properties:

- Trust is not *Transitive*; if I trust Alice and Alice trusts John, that does not mean I should trust John. Essentially, trust relationship between two entities is a *vector* that consists of trust value in conjunction with direction.
- Trust is *Contextual* [7]. A truster may have different and independent sets of trust relationships given her different roles or configurations. For example, a person can be a tourist, a hobbyist, an employee, a father, a husband, a consultant, a teacher or a

volunteer, to name a few; a mobile device may be used in a security zone with restrictions or in a public place playing games. Trust relationships vary depending on such situations that arise from these contexts.

- Trust is *Granular*. Trust is an assessment of many trust-related distinct scores taken from the evidences provided, not just one cumulative and global score value.
- Trust is *Belief-based*. Different truster's have different beliefs of trust. Some trust until trust is broken; others distrust until trust is earned.
- Trust assessment is *Situational*. Which context applies to the question of "Do I trust?" depends on the situation.
- Trust assessment is *Intent-driven*. A situation defines the context, but the intent defines the trust scoring.
- Trust is *Continuously Reevaluated*. Yesterday one may trust, today they do not, while tomorrow they will again. Why? Situations, contexts, and evidence. Scores change based on continuous assessment of the trustee's relationships – Dynamic Trust Establishment. A trust-based paradigm shift takes the blind trust method and introduces a trust query allowing both the client and the server to proceed based on their latest and up-to-date understanding of the trust relationship between the two entities (as shown in Figure 1 below). In such a methodology, the trust is a property that leverages dynamic verification and updates for such trust relationships, taking contexts, and entity specific (e.g., personal) policies into account.

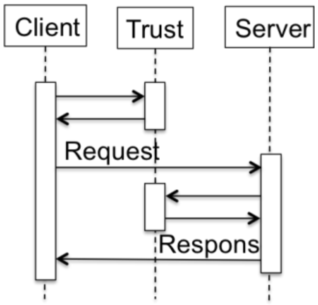


Figure 1. Dynamic Trust between client and a server

B. Entities

Entities are the objects between which trust is established and maintained. An *entity* is defined as any person, place, or thing with a distinct and independent existence that may trust or be trusted.

Each entity needs to be uniquely identified. One possible identification mechanism may be the *Extensible Resource Identifier* as defined by the XRI [8] Technical Committee at OASIS.

As shown in Figure 2 below, entities have a duality as either:

- a *truster* which positions the entity as the one that is trusting another (i.e., a trustee), or
- a *trustee* which positions the entity as the one that is being trusted by a truster.

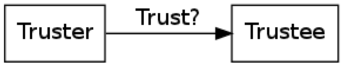


Figure 2. Trusters and Trustees

Trusters have a belief policy and one or more contexts.

C. Truster Contexts and Situations

Truster contexts are a way to partition an entity's singular notion of trust into different sets of related trust domains. To answer questions of trust, one first has to establish the context. The specific contexts are selected based on specific *situations* that are present at the time of trust determination. Consider, as an example, the many contexts that a person can be a part of, as the example in the Figure 3 below illustrates. All these examples are contexts. These differentiate in how a truster evaluates trust or risk assessment.

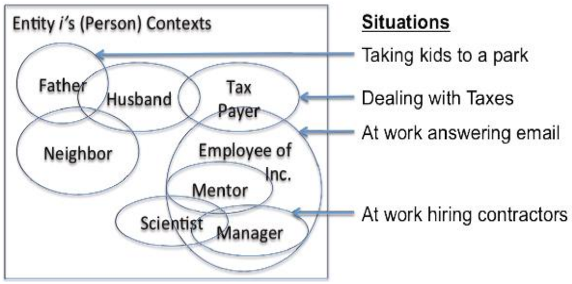


Figure 3. Examples of situations that select which truster's context applies to those situations

D. Belief Policies and Intent

Context and situations alone are not sufficient to assess trust. Each entity must be able to apply its own belief in trust assessment. A *Belief Policy* can be defined that helps determine how trust values are interpreted to derive a Boolean trust value for a specific scenario. A final trust score of 0.8 may signal one to trust but another not to. Belief Policies maintain trust value thresholds, and allow the entity to change its belief over time as trust is gained or reduced.

In addition to the Belief Policy, the intent of the situation has to also be taken into account. Consider an example. A situation in which a person is at work on Monday talking to a non-employee in a conference room with a human resources representative present may identify the context as that of an interview. But the interviewers (truster) intent may affect the trust determination of the interviewee (trustee). If the interviewer's intent is to hire a friend its risk acceptance is higher and so is his trust. If the interviewer's intent is to hire a replacement, their trust may be lower. Thus, intent is an adjustment to one's belief policy is important in allowing for more accurate trust assessment of a given context identified by a specific situation.

III. Trust Management System Overview

The following schematic as shown in Figure 4 below captures details for the *Trust Management System* as a whole. Subsequent subsections describe all these components in more detail.

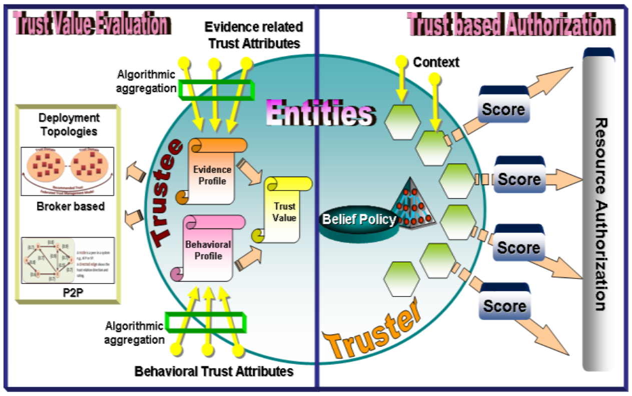


Figure 4. Trust Management System Overview

A. Trust Value Evaluation

As mentioned in the introduction, in a highly de-centralized environment, the contemporary static role assignment mechanism needs to be evolved in such a manner that it enables a dynamic trust value assignment to a *trustee* entity. Trust based authorization mechanism, in turn, leverages the dynamic trust value assigned to the *trustee* entity and makes the access control decisions accordingly in a highly dynamic manner.

Trust Value Evaluation process essentially entails collecting the relevant information necessary to establish trust relationship and, at the same time, dynamically monitors and adjusts the existing trust relationship. This process assigns a single-valued scalar numeric value in the range [0..1]. Lower trust value signifies lack of trust, while higher value denotes more trustworthiness of an entity. A trust value of 0 represents the condition with the highest risk for an entity and 1 representing the condition that is totally risk-free or fully trusted.

As mentioned earlier, trust is always related to a particular context. An entity A needs not trust another entity B completely. Entity A only needs to calculate the trust associated with B in some context pertinent to a situation. The specific context will depend on the nature of application and can be defined accordingly. Based on our current model, trust is evaluated under a single context only.

Trust Value for an entity is determined by a combination of the following two models:

- ***Evidence-based*** model, an appropriate trust value is assigned to an entity based on some evidence such as self-defense evidence etc. explicitly manifested by the entity.
- ***Reputation-based*** model [9][10][11]12], in which Direct Experience coupled with Indirect Recommendation/s establishes the trust value of an entity.

Based on these two criteria, the trust rating value could be obtained by applying different mathematical functions/algorithms to all the relevant trust attributes applicable for an entity. All of the trust attributes (*Evidence-based* as well as *Reputation-based* attributes) would be assigned respective weights as part of the trust calculation algorithm.

The following three sub-sections describe brief summary of various trust value evaluation models. These sub-sections provide general foundation and grounding for these models and complexities involved. As part of our future work, we will delve deeper as far as describing the actual mathematical algorithms/functions and in-depth technology details for these trust value evaluation models.

1) Evidence-based Trust Model

In the ***Evidence-based*** model, trust is considered as a set of relationships established with the support of evidence. Evidence can be anything a policy requires to establish a trust relationship, such as attendance list, annual report, or access history. For example, in case of a web service resource, the intrinsic trust value calculation algorithm may factor in web service attributes such as:

- <u>Dependability</u> characteristics such as Accessibility, Availability, Accuracy, Reliability, Capacity, Flexibility etc.
- <u>Self-Defense</u> characteristics such as Authentication, Authorization, Non-repudiation, encryption, privacy, Anti-Virus Capabilities, Firewall Capabilities, Intrusion Detection Capabilities etc.
- <u>Performance</u> characteristics such as Latency, Throughput etc.
- and much more …

2) Reputation-based Trust Model

In the ***Reputation-based*** model, on the other hand, trust is motivated from human society, where human beings get to know each other via direct interaction and through a grapevine of relationships. In a large distributed system, every entity can not obtain first-hand information about all other entities. As an option, entities can rely on second-hand information or recommendations. Reputation is defined as “perception that an entity creates through past actions about other entity’s intentions and track record”.

The reputation assessment of an evaluated entity by an evaluator entity involves collecting information such as:

- *<u>Direct Trust</u>*, the evaluator’s own interaction experiences with the evaluated entity; if the evaluator entity has first-hand experience of interacting with evaluated entity in the past.
- *<u>Recommender Trust</u>*, recommendation from peers who have interacted with the evaluated entity before. Attributes such as *Prior Success Rate*, *Turnaround Time*, *Cumulative Site Utilization* etc. are few examples of Reputation trust. Time is the key dimension for reputation. Reputation builds with time – reputation enhances or decays as the time goes by.

The recommendation protocol is straightforward. For example, entity A needs a service from entity D. A knows nothing about the quality of D’s service, so A asks B for a recommendation with respect to the service category, assuming that A trusts B’s recommendation within this category. When B receives this request and finds that it doesn’t know D either, B forwards A’s request to C, which has D’s trustworthiness information within the service category. C sends a reply to A with D’s trust value. The path (A)X(B)X(C)X(D) is the *recommendation path*. When multiple recommendation paths exist between the requester and the target, the target’s eventual trust value may be the average of the values calculated from different paths.

As mentioned earlier, *Time* is the key dimension for reputation. As in relationship, trust may decrease with time. For example, if an entity has not interacted with another entity for some time, then the trust value between these two entities is likely to be weaker. To account for *Time* dimension, a *time decay factor* needs to be included as part of the trust calculation algorithm.

3) Trust Normalization Policy and Unit of Measure (UOM) Standardization

As mentioned earlier, all of the trust attributes (*Evidence-based* as well as *Reputation-based* attributes) would be assigned respective weights as part of the trust calculation algorithm. However, lack of a *standard unit of measure* for quality of these attributes may pose a huge challenge. Also, without trust normalization policy, it would be difficult to deterministically determine the weights and the correct set of attributes to be included at the time of trust value calculation process. Such a *deterministic* approach would be a daunting task, nonetheless.

During evaluation of a trust value, a truster may assign different weights to the different factors that influence trust. The weights will depend on the trust evaluation policy of the truster. So, if two different trusters assign two different sets of weights, then the resulting trust value will be different. The trust normalization policy addresses this particular issue. The trust normalization policy to go along with the *Evidence-based* model and *Reputation-based* model forms the complete *truster’s* trust evaluation policy.

B. Trust Management Topologies

The previous section explains all the complexities of determining trust value of an entity. There are primarily two topologies to support such a trust value evaluation process.

- A centralized broker-based trust aggregation topology.
- A trust overlay network based peer-to-peer decentralized topology.

Whether a trust topology is centralized or decentralized determines the feasibility and complexity of a trust value evaluation mechanism. In a centralized system, a central node will take all the responsibilities of managing reputations for all the members. In a decentralized system, e.g., a peer-to-peer system, there is no central node. The members in the system have to cooperate and share the responsibilities to manage reputation.

Generally speaking, the mechanisms in centralized systems are less complex and easier to implement than those in decentralized systems. But, they need powerful and reliable centralized servers and a lot of bandwidth for computing, data storage, and communication.

The following two sub-sections give a brief summary of these two topologies. These sub-sections provide general foundation and grounding for various topologies and complexities involved. As part of our future work, we will delve deep as far as describing the actual in-depth mathematical algorithms/functions and technology details for these deployment topologies.

1) Trust Broker Topology

As shown in Figure 5 below, in a centralized broker-based [13] trust aggregation topology, the entire trust landscape is divided into trust domains. Trust agents/entities inherit the trust properties of the domain they are associated with. This increases the scalability of the overall approach.

Trust entities rely on the trust broker to manage trust. As Domain trust agents, trust brokers store other domain’s trust information for inter-domain cooperation. Essentially, the trust information stored reflects trust value for a particular resource type (compute, storage, etc.) for each domain. Trust Brokers also recommend other domains trust levels for the first time inter-domain interaction.

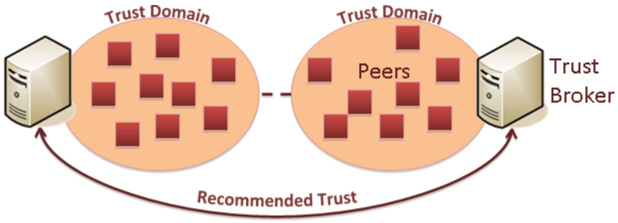


Figure 5. Trust Broker based Federated Trust Management Topology

A decentralized Distributed Hash Table (DHT) based 3rd Party Trust Management may be used for efficiently managing various trust domains. Individual entities themselves do not need to take any responsibilities for managing the trust model. Instead, the responsibility is delegated to the 3rd party trust broker node. However, this approach has classical disadvantages of a typical centralized methodology – performance bottlenecks, single point of failure etc.

2) P2P Topology

Peer-to-Peer (P2P) Trust Management topology [14][15][16][17], on the other hand, does not employ any centralized server. As shown in Figure 6 below, each peer maintains a local trust table to store trust information of neighboring nodes. Trust Vector Aggregation Algorithm can infer indirect trust among peers. Each member entity itself has to cooperate and share responsibilities to manage the local level trust index. Trust value for all nodes is determined algorithmically.

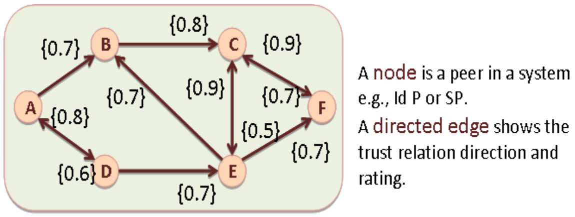

{0.8}
{0.7}
B
C
{0.9}
A
{0.7}
{0.9}
{0.7}
F
{0.8}
{0.5}
{0.7}
{0.6}
D
E
{0.7}
A node is a peer in a system e.g., Id P or SP.
A directed edge shows the trust relation direction and rating.

Figure 6. P2P Topology

In such a decentralized environment, finding *Most Trustable Path* so that the trust path yields the highest trust value from thousands or millions of peers is a mammoth challenge, to say the least. Also, trust propagation to each peer in a vast network of peers is yet another challenge that needs to be addressed as part of the overall Peer-to-Peer (P2P) topology.

C. Trust based Authorization

As stated earlier in the introduction section, in an open and highly decentralized environment where entities are dynamic in nature, the identity of every entity is not known in advance. In such an environment, the static role assignment needs to be evolved in such a manner that it enables a dynamic trust value assignment to a *trustee* entity. Trust based authorization mechanism, in turn, leverages the dynamic trust value assigned to the *trustee* entity and makes the access control decisions accordingly in a highly dynamic manner. As mentioned earlier, the *truster* decides permissions based on Principle's set of attributes instead of principle's identities. Trust attributes may include *Evidence-based* as well as *Reputation-based* attributes as covered in the previous section.

In very simplistic terms, *Trust based Authorization* process is a mathematical equation. On one side of the equation is the *Security Demand* (**SD**) of an entity. On the other side of the equation is the *Trust Value* (**TV**) that reveals of another entity. These two must satisfy a security assurance condition so that ***TV*** >= ***SD***.

As mentioned earlier, trust relationship between two entities is a *vector* and is always related to a particular context. The trust vector is a vector of trust value and trust direction, where trust value is defined as a real number in the range [0..1] and direction is defined as a directed edge in the trust graph. The edge in a graph represents the rating for a combination of all direct transactions between two peers. Trust value itself is composed of three key components – Evidence, Direct Experience, and Recommendations from others. As shown in equation (1) below, trust relationship between entity A and B in simple terms can be described as:

$$TV(A \rightarrow^{c} B) = [{}_{A}E^{c}_{B,}\ {}_{A}D^{c}_{B,}\ {}_{O}R^{c}_{B}] \qquad (1)$$

Here the value ${}_{A}E^{c}_{B}$ represents the level of evidence demonstrated by entity B to entity A under context c. The value ${}_{A}D^{c}_{B}$ represents the magnitude of direct experience of entity A in relation to entity B under context c. The value ${}_{O}R^{c}_{B}$ represents the cumulative effect of all recommendations from all other entities for entity B under context c. Each of these three components is expressed in terms of a numeric value in the range [0..1].

We propose a XACML-compliant policy management system as part of the trust based authorization scheme. XACML provides a standardized language and method of access control and policy enforcement.

eXtensible Access Control Markup Language (XACML) [18] is an XML-based language for access control that has been standardized in OASIS. XACML describes both an access control policy language and a request/response language. The policy language is used to express access control policies (who can do what when). The request/response language expresses queries about whether a particular access should be allowed (requests) and describes answers to those queries (responses).

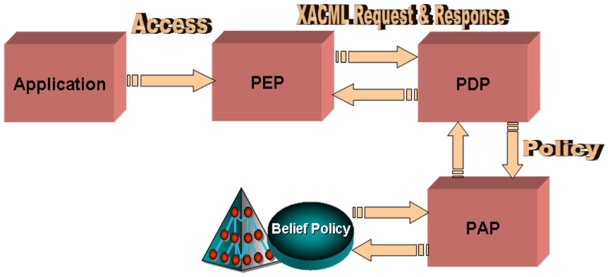


Figure 7. OASIS XACML Authorization Environment

In a typical XACML usage scenario, a subject (e.g. human user, device) wants to take some action on a particular resource. As shown in Figure 7 above, the subject submits its query to the entity protecting the resource. This entity is called a Policy Enforcement Point (PEP). The PEP forms a request (using the XACML request language) based on the attributes of the subject (trust value in our case), action, resource, and other relevant information. As shown in Figure 8 below, the PEP then sends this request to a Policy Decision Point (PDP), which examines the request, retrieves policies (written in the XACML policy language) that are applicable to this request, and determines whether access should be granted according to the XACML rules for evaluating policies. That answer (expressed in the XACML response language) is returned to the PEP, which can then allow or deny access to the requester. Policy Administration Point (PAP) is used to get to the policies; the PDP uses the PAP where policies are authored and stored in an appropriate repository.

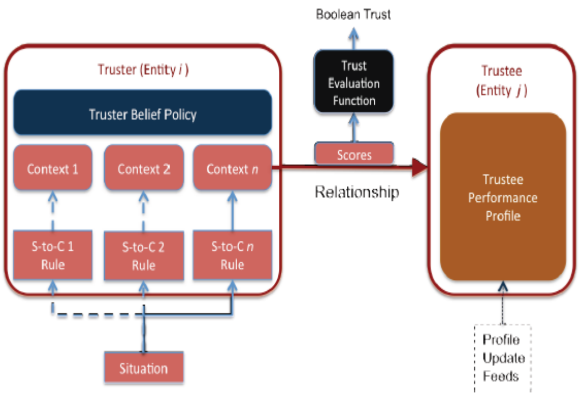


Figure 8. Trust based Decisioning Process

In this section, we described a brief summary of trust based authorization framework. The section provided general foundation and grounding for various complexities involved.

D. *Trust Management Conceptual Layered Architecture*

As shown in Figure 9 below, the key ingredients of the conceptual architecture are:

- *Trust Rating Layer*
- *Trust Aggregation Layer*
- *Trust Access Layer*

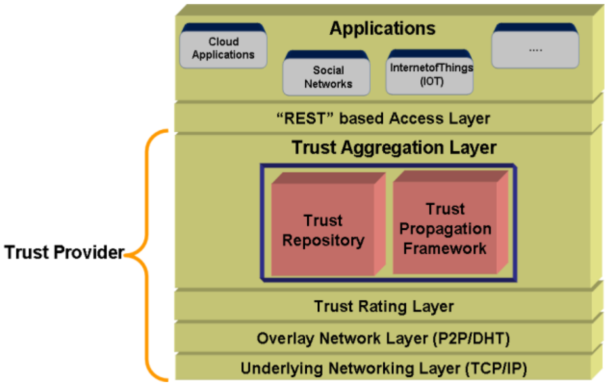


Figure 9. Trust Management Conceptual Architecture

The details for *Trust Rating Layer* have already been described earlier, as part of the ***Trust Value Evaluation*** section.

Trust Aggregation Layer is responsible for aggregation of distributed trust scores in a peer-to-peer environment. It is based on mathematical algorithm for fast and lightweight trust score aggregation.

Trust Access Layer provides entities to extract trust information from the trust model. This REpresentational State Transfer (REST) API specification is for the interface of the Trust System. The API set consists of methods related to:

- Entities (Create, List, Find, Entity Details, Modify, Delete)
- Entity Context (Create, List, Find, Entity Details, Modify, Delete)
- Entity Belief Policy (Get, Modify)
- Entity Relationship (Create, Find, List, Get, Modify)
- Trust Determination
- etc.

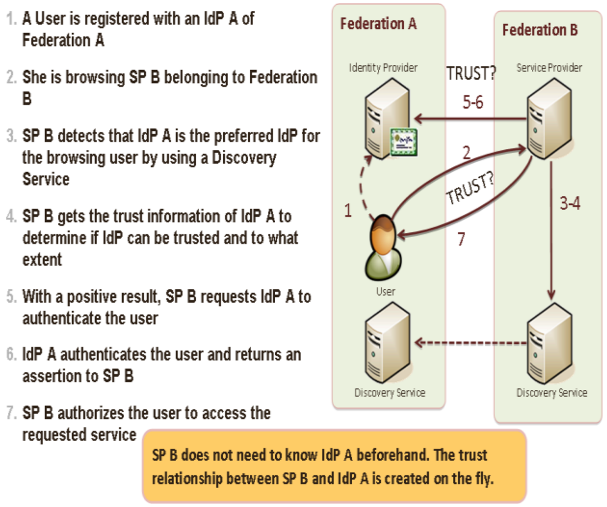
IV. Trust Management – Use Cases

This section enumerates various business use case scenarios articulating how such a *Trust Management* framework would be invaluable for addressing the current as well as future computing environment needs. The following are few of the business use cases in which the proposed *Trust Management* framework can play a huge role as part of the next generation highly distributed computing environment.

A. *NextGen Trust aware Federated Identity Management*

Federated Identity Management has existed for a while. However, almost all existing approaches to identity federation are based on static relationships. In a static federation, relationships among identity providers (IdPs) and *Service Providers* (SPs) are manually pre-configured in their metadata repository. The question of whether an entity can trust another depends on if they can find each other in the pre-wired metadata repository, thus this question cannot be answered in a dynamic manner due to the static nature of the meta data.

Current *Federated Identity Management* solutions lead to problems with scalability and deployment in real-time dynamic environment such as mobile networks and *Internet of Things* in general. Firstly, every new relationship between any two entities must be added manually as such a static federation cannot be quickly and easily expanded to accommodate hundreds, thousands or even millions of IdPs and SPs nodes. In essence, a static *Identity Federation* cannot be deployed in a real-time environment like a mobile network or in *IoT* environment where devices may potentially access each other across federation boundaries and at any time.



1. A User is registered with an IdP A of Federation A
2. She is browsing SP B belonging to Federation B
3. SP B detects that IdP A is the preferred IdP for the browsing user by using a Discovery Service
4. SP B gets the trust information of IdP A to determine if IdP can be trusted and to what extent
5. With a positive result, SP B requests IdP A to authenticate the user
6. IdP A authenticates the user and returns an assertion to SP B
7. SP B authorizes the user to access the requested service

SP B does not need to know IdP A beforehand. The trust relationship between SP B and IdP A is created on the fly.

Figure 10. Trust aware Federated Identity Management

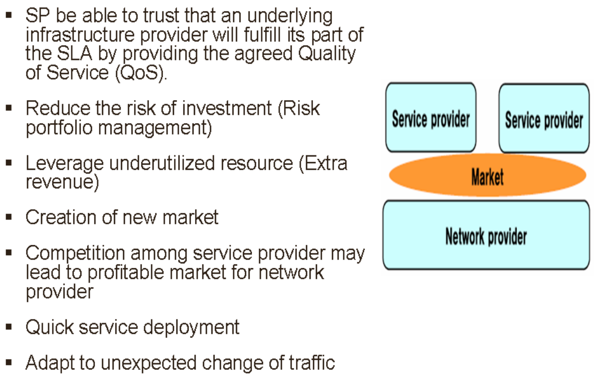
The proposed *Trust Model* enables a dynamic federation environment, in which the IdPs and SPs will be regarded as peers of a trusted network that evolves over time. A trust relationship between two entities is regarded as a network connection. As shown in Figure 10 above, in such a dynamic federation, an SP does not need to know an IdP beforehand. A trust relationship will be created on demand and the trust value, namely how much an IdP can be trusted will be determined on the fly.

B. *Trust aware Network Virtualization*

Network Virtualization enabled Bandwidth Trading - Most network traffic does not flow in steady and easily predictable streams, but in short bursts, separated by longer periods of inactivity. This pattern makes it difficult to predict peak loads. *Bandwidth on Demand* is useful for applications, such as backups, files transfers, synchronization of data bases, and videoconferencing, and allows the user to pay for only the amount of bandwidth used. It is a technique that allows the user to add additional bandwidth as the application requires it.

Traditionally, in a network virtualization environment, trust, if addressed, is generally addressed from the security and privacy point of view only. Authentication, authorization, access control, ensuring integrity of information and protecting the source of information are used to provide a secure virtual network. However, there are other trust related aspects that need to be taken into consideration. For example, we should be able to trust that an underlying infrastructure provider will fulfill its part of the SLA by providing the agreed Quality of Service (QoS).

A SP assesses the quality of service of an infrastructure network provider involved in a virtual network in terms of availability of resources, reliability, confidentiality and integrity, and adaptability to network conditions. The feedbacks sent by different *Service Providers* are gathered and stored. A *Trust Management Service* is used to keep track of trust data of infrastructure providers. As shown in Figure 11 below, while mapping a virtual network, the SP will take into consideration the reputation of the infrastructure providers.



- SP be able to trust that an underlying infrastructure provider will fulfill its part of the SLA by providing the agreed Quality of Service (QoS).
- Reduce the risk of investment (Risk portfolio management)
- Leverage underutilized resource (Extra revenue)
- Creation of new market
- Competition among service provider may lead to profitable market for network provider
- Quick service deployment
- Adapt to unexpected change of traffic

Figure 11. Trust aware Network Virtualization

Mapping a virtual network request requires the selection of specific nodes and links according to the requirement of a *Service Provider* in terms of resources (e.g., location and CPU of the nodes, and the bandwidth of the links) and cost. If *Service Providers* consider only the cost, the infrastructure providers may be tempted to reduce the price by minimizing the quality of the physical underlying network.

To make the right decisions, trust information of the infrastructure providers is taken into account while performing a Virtual Network (VN) mapping. Avoiding un-trusted physical network providers, where failure of nodes and links could easily happen, will improve the service provided to the users. *Service Providers* may reward reputable infrastructure providers by higher priority/probability of involvement in future VN mapping requests.

C. *Trust Model for Device Mobility*

There is a need for Trust-based Mobile Device Control Management for Enterprises

- Mobile devices are set up for only one security domain with static access policy limit usability and increases costs.
- Enterprises are adopting hybrid public/private cloud services.
- Enterprise security needs must balance personal privacy needs and usability.
- Enterprises must accept the coexistence of personal and corporate apps and data.
- Enterprises can adopt dynamic and real-time control policies based on managing risk with trust.
    - Granular Trust Attributes are defined for users, devices, apps, etc.
    - Trust is learned and continually verified and adjusted.
    - Trust is mutual and bi-directional, so are the policies.

V. Conclusions and Future Work

In this paper, we described various components of the *Trust Management* system in great detail and strived to provide a general foundation for building various constituents of the trust system. However, it does not delve deep as far as describing the actual mathematical algorithms/functions and in-depth technology details for underlying components. Our future work will publish such in-depth details for each and every components of the *Trust Management* system.

In order to make this a reality, an operational trust management system must be experimented with in a live public trial. To that regard, we are working towards establishing the *Trust Management Testbed* by collaborating with various well known academic institutions and industry leaders.

Acknowledgment

We would like to thank:

- Farag Azzedin & Muthucumaru Maheswaran of University of Manitoba and TR*Labs* Winnipeg, Manitoba, Canada, for their work on “Evolving and Managing Trust in Grid Computing Systems”.
- Huaizhi Li and Mukesh Singhal of University of Kentucky for their work on “Trust Management in Distributed Systems”.

REFERENCES

[1] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability, in Proceedings of ICIW '09, the Fourth International Conference on Internet and Web Applications and Services, 2009, pp. 328-336.

[2] R. Buyya, S. Pandey, and C. Vecchiola: Cloudbus toolkit for market-oriented cloud computing, in Proceedings of 1st International Conference on Cloud Computing (CloudCom), 2009.

[3] D. Bernstein and D. Vij, Intercloud Exchanges and Roots Topology and Trust Blueprint, in Proceedings of the IEEE 2011 International Conference on Internet Computing, Las Vegas, USA, 2011.

[4] E. F., Chrchill, On Trust Your Socks to Find Each Other, Yahoo Interactions, March 2009.

[5] K. Thompson, Reflections on Trusting Trust, Communications of the ACM, August 1984.

[6] L. J. Hoffman, K. Lawson-Jenkins, and J. Blum, Trust Beyond Security: An Expanded Trust Model, Communications of the ACM, July 2006, 49(7):94-101.

[7] M. C Huebscher and J. A McCann, A Learning Model for Trustworthiness of Context-awareness Services, Proceedings of the 3rd Int’l Conf. on Pervasive Computing and Communications Workshops, 2005, pp. 120-124.

[8] OASIS Extensible Resource Identifier (XRI) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xri, [retrieved: December, 2013].

[9] J. Goldbeck and J. Hendler, Inferring Reputation on the Semantic Web, in Proceedings of the 13th International World Wide Web Conference, May 2004.

[10] F. G. Marmol and G. M. Perez, Security threats scenarios in trust and reputation models for distributed systems, Elsevier, Computers & Security 28, 2009, pp. 545-556.

[11] S. Ramchurn, C. Sierra, L. Godo, and N. Jennings. Devising a trust model for multiagent interactions using confidence and reputation, International Journal of Applied Artificial Intelligence, 2005, 18(9–10):91–204.

[12] J. Goldbeck, Semantic Web Interaction through Trust Network Recommender Systems in end user semantic web interaction workshop at the 4th international semantic web conference, 2005.

[13] K-J. Lin, H. Lu, T. Yu, and C. Tai, Reputation and Trust Management Broker Framework for Web Applications, in e-Technology, e-Commerce and e-Service, 2005. EEE '05, The 2005 IEEE International Conference, 2005.

[14] R. Zhou and K.Hwang, Trust Overlay Networks for Global Reputation Aggregation in P2P Grid Computing, *IEEE IPDPS*, 2006.

[15] T. Repantis and V. Kalogeraki, Decentralized Trust Management for Ad-Hoc Peer-to-Peer Networks, ACM MPAC, 2006.

[16] S. Ayyasamy and S. N. Sivanandam, Trust Based Content Distribution for Peer-to-Peer Overlay Network in International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010.

[17] G. H. Nguyen, P. Chatalic, and M. C. Rousset, A Probabilistic Trust Model for Semantic Peer to Peer Systems, *DAMAP ’08,* March 2008.

[18] OASIS xEtensible Access Control Markup Language (XACML) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml, [retrieved: December, 2013].

Analysis of Power Consumption of H.264/AVC-based Video Sensor Networks through Modeling the Encoding Complexity and Bitrate

Bambang A.B. Sarif, Panos Nasiopoulos and Victor C.M. Leung
Department of Electrical and Computer Engineering,
University of British Columbia
Vancouver, Canada
{bambangs, panosn, vleung}@ece.ubc.ca

Mahsa T. Pourazad
Department of Electrical and Computer Engineering,
University of British Columbia
TELUS Communications Inc.
Vancouver, Canada
pourazad@ece.ubc.ca

***Abstract*—The H.264/AVC video encoding standard has many advanced features that can be tailored to suit a wide range of applications. In order to obtain optimal coding performance in video sensor networks (VSNs), it is essential to find the right setting parameters for the encoder. There is a trade-off between required energy for encoding and transmission of video content in VSNs that can be exploited to minimize total power consumption. In this study, we model the complexity and bitrate in H.264/AVC codec. By using the model, the trade-off between encoding and transmission energy consumption is further exploited. Our experiments show that the complexity modeling error is less than or equal to 3.45%. However, the bitrate modeling error that we obtain is less than or equal to 11.6%.**

Keywords-H.264/AVC; complexity and bitrate modeling; energy consumption model; and video sensor network

I. Introduction

With the increasing concern about security in homes or public spaces, the demands for monitoring and surveillance systems is growing. In this regard, video sensor networks (VSNs) offer an alternative to several existing monitoring technologies [1], [2]. However, unlike the traditional sensor networks which require negligible power to process captured data in the sensor nodes, VSNs need significant processing power to encode and transmit the captured videos. With the limitations of energy resources in VSNs, maximizing the power efficiency of coding and transmission operations becomes very important. In general, there is a tradeoff between encoding complexity and compression performance in the sense that to obtain higher compression performance (i.e., lower bit rate), more complex and computationally expensive encoding scheme is required. On the other hand, transmission of lower bitrate content requires less amount of energy. Fig. 1 illustrates the relationship between coding complexity, compression performance and the required power for encoding and transmission of the content. It can be observed that, to minimize the overall VSN power consumption, encoding process needs to be handled carefully. Among the existing video coding standards, H.264/AVC is the most widely used standard in the consumer market [3], [4]. Some of the existing studies on the performance of H.264/AVC codec look into maximizing the coding performance without considering the total power consumption of the coding process [3], [5]. J.J. Ahmad et al. [6] studied the required energy for encoding and transmission of video content in the case of using H.264/AVC codec. Unfortunately, the number of configuration settings considered for the encoder in that study is limited. To address this issue, we extended the study in [6] by including more encoder configuration settings in our previous work [7]. We proposed a guideline table for encoder configuration setting which include different combinations of coding complexity and coding efficiency in terms of bitrate that produces compressed videos with similar quality in terms of peak signal to noise ratio (PSNR). Our study shows that the energy consumption of a VSN can be reduced by carefully selecting the encoder settings at each VSN node based on the proposed table.

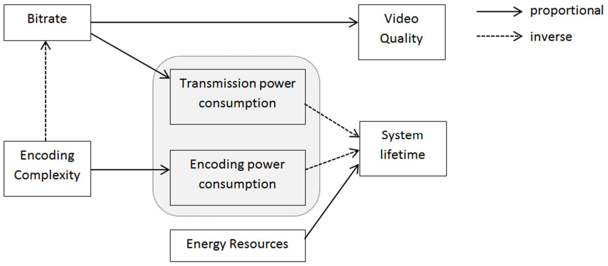


Figure 1. Relation between encoding and transmission power consumption

This paper is an extension to our previous work [7] where the relationship between coding complexity and coding efficiency (in terms of bitrate) of H.264/AVC codec is modeled. By using this model, the trade-off between encoder complexity and bitrate can be further elaborated, unrestrained with the encoder setting parameters. The rest of the paper is organized as follows. Section II describes the H.264/AVC encoding complexity and bitrate modeling. The encoding and transmission power consumption model is then discussed in Section III. Conclusions are drawn in Section IV.

ISBN: 978-1-61208-324-7

II. H.264/AVC Complexity and Bitrate Modeling

H.264/AVC is a block-based hybrid video coding standard utilizing intra-frame and inter-frame prediction. While inter-frame prediction is more involved than intra-frame prediction, it results in lower bitrate. By increasing the number of inter-frames coded picture within a successive video stream, i.e., group of picture (GOP) size, the bitrate of the coded video is reduced at the cost of higher encoding complexity. In the case of inter-frame prediction, the complexity and bitrate can be controlled by adjusting the search range (SR) in motion estimation process. The SR determines the size of searching area in the reference frame to find the best match to be used for inter prediction. Increasing the SR size may result in better compression performance at the cost of increased complexity. However this observation is quite content dependant and there are cases where increasing the value of SR does not provide significant benefit in terms of compression performance [7].

The other factor that controls the complexity and the performance of the H.264/AVC codec is the number of block sizes used in the inter prediction process. Increasing the number of used block sizes results in better prediction and consequently higher compression performance at the expense of increased complexity. The complexity of motion estimation (ME) can be classified into different level of complexity, depending on the number of block size candidates used. In general, there are seven block sizes defined for inter-prediction in H.264/AVC.

In this paper, we analyze the effect of different coding parameters on the coding complexity using a set of training videos and propose a model for the relationship between coding configuration and coding complexity, and later this model is tested on a set of unseen test video set. The following subsections provide more details on our experiment settings and the proposed model.

A. Experiment Settings

In VSN applications, due to the limitations in energy and processing resources, less complex encoder configurations are used. To this end, we used baseline profile of H.264/AVC that is suitable for low complexity applications and uses only I and P frames (no B-frames) in our study. The other encoding parameters in our experiments include using context-adaptive variable-length coding (CAVLC) entropy coding and one reference frame, setting SR equal to 8, and disabling the rate distortion optimization (RDO), rate control, deblocking filter and Intra coding for P frames options. Furthermore, to have an objective measure for the encoding complexity, we use the instruction level profiler *iprof* [8], which provides us with the total number of instruction counts. The H.264/AVC reference software, JM version 18.2 is used in our experiments. Five representative videos from [9] are used in our study (BQMall, Traffic, Race Horse, PeopleOnStreet and Vidyo1). To mimic a common VSN data, these sequences are downsampled to the common intermediate format (CIF) resolution (352x288 pixels) and also their frame rate was reduced to 15 frames per second (fps). The BQMall and Traffic video sequences are used as the training set for the model and the rest of videos as the test set.

TABLE I
ME Complexity Level (M_L)

M_L	***Block Size Candidates***
1	SKIP, 16X16
2	SKIP, 16X16, 16X8
3	SKIP, 16X16, 16X8, 8X16
4	SKIP, 16X16, 16X8, 8X16, 8X8
5	SKIP, 16X16, 16X8, 8X16, 8X8, 8X4
6	SKIP, 16X16, 16X8, 8X16, 8X8, 8X4, 4X8
7	SKIP, 16X16, 16X8, 8X16, 8X8, 8X4, 4X8, 4X4

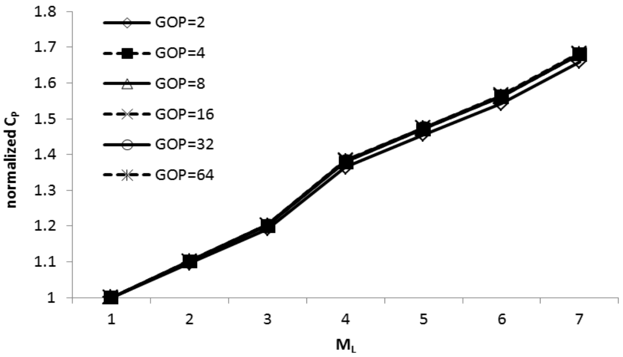


Fig. 2. Normalized C_P for different M_L for "BQMall" video

B. Complexity Modelling

The coding process complexity of a video sequence (C_S) is formulated as follows:

$$C_S = C_I \cdot n_I + C_P \cdot n_P \tag{1}$$

where C_I is the complexity to encode an I-frame, C_P is the complexity to encode a P-frame, n_I is the number of I-frames in the sequence and n_P is the number of P-frames in the sequence. For a video sequence with no scene change, the value of C_I can be considered almost constant. On the other hand, C_P depends on the complexity level of the ME process. In our study, the complexity level of ME process (called M_L) is classified based on the used block-size candidates in the encoding process as shown in Table I.

As illustrated in Fig. 2, the GOP size does not affect the normalized coding complexity of P frames at each M_L. Note that the complexity of coding P-frame (C_P) is normalized with respect to C_p when M_L is equal to one. Furthermore, as it can be seen from Fig. 3, the plot of normalized C_P for different training videos has the same slope but scaled by a constant. It can be seen from this figure that the normalized C_P for the Traffic video ranges from 1 to 1.485, which also

TABLE II
ME COMPLEXITY LEVEL (M_L) AND δ_{CP}

M_L	δ_{CP}
1	0
2	0.13
3	0.26
4	0.54
5	0.67
6	0.81
7	1

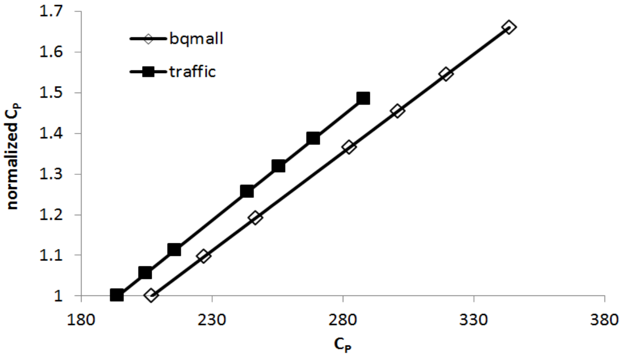


Fig. 3. Normalized C_P for GOP=2 of the training videos

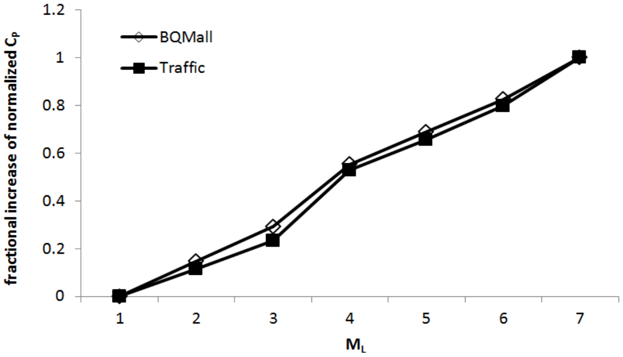


Fig. 4. Fractional increase of normalized C_P for the training videos

means that the normalized C_P range for this video is 0.485. On the other hand, the normalized C_P range for the BQMall video is equal to 0.66. Scaling the range of the normalized C_P to one, we can plot the fractional increase of normalized C_P as shown in Fig. 4. It is interesting to see that the increase of normalized C_P with respect to M_L is almost similar for both videos. We define δ_{CP} as the amount of increase normalized C_P at different M_L. δ_{CP} is calculated by averaging the values obtained in Fig. 4, as shown in Table II.

Another interesting observation is that, the value of range of normalized C_P shown in Fig. 2 is proportional to the value of $Cp_{M_L=1}$. Therefore, using the values obtained from the training videos, the range of normalized C_P values for a specific video sequence is calculated as:

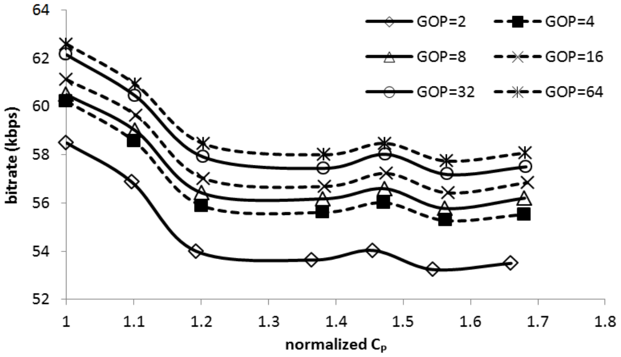


Fig. 5. Bitrate of a P-frame for different M_L of "BQMall" video

$$\omega_I = 0.0135 \cdot Cp_{M_L=1} - 2.13 \qquad (2)$$

Using ω_I, the complexity to encode a P-frame is formulated as:

$$Cp_{M_L=i} = Cp_{M_L=1} \cdot \left(1 + \delta_{CP}(i) \cdot \omega_1\right) \qquad (3)$$

Considering that n_I=N/GOP, where N is total number of frames and n_P=N–N/GOP, then the average complexity per frame is computed as follows:

$$C_f = (C_I + Cp_{M_L=1} \cdot (1 + \delta_{CP} \cdot \omega_1) \cdot (GOP - 1)) / GOP \qquad (4)$$

C. *Bitrate Modelling*

The bitrate of the encoded video is modeled as R=$R_f \cdot F_r$, where R_f is the average bitrate of a frame and F_r is the frame rate. The total size of the encoded sequence (in bit) is then modeled as:

$$R_S = R_I \cdot n_I + R_P \cdot n_P \qquad (5)$$

where R_I is the average size of an I-frame and R_P is the average size of a P-frame. The value of R_P depends on the M_L and GOP used by the encoder.

Fig. 5 shows that, the value of R_P decreases as M_L increases. Therefore, for a certain GOP value, the R_P is modeled as:

$$R_{P_{GOP=i}} = \omega_{Ri} \cdot f(M_L) \qquad (6)$$

where ω_{Ri} is the bitrate of a P-frame when GOP=i and M_L=1, and $f(M_L)$ is a decay function with respect to M_L, which is modeled using the generalized logistic function. The logistic function is a widely used sigmoid function for growth/decay modeling where the growth/decay is exponential at first, but eventually slower and then levels off. This matches the way R_P is reduced with the increase of

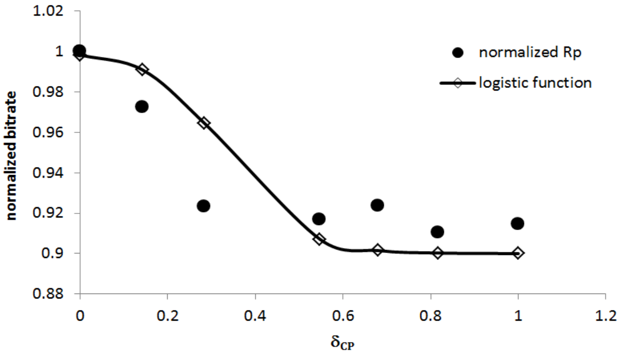


Fig. 6. The normalized bitrate ("BQMall", *GOP*=2) and the logistic function

M_L (see Fig. 5). The logistic function *f(M$_L$)* used in our study is as follows:

$$f(M_L) = a + \frac{b-a}{1+e^{-c(x-d)}} \qquad (7)$$

where *a* and *b* indicate the minimum and maximum asymptote of the plot respectively, *c* is the growth rate, while *d* signify the time for maximum growth (see Fig. 6).

Furthermore, Fig. 5 also shows that the slope of the R_P plot for different *GOP* sizes is the same. Therefore, R_P is modeled equal to:

$$R_P = \omega_{Rp} \cdot f(M_L) + \omega_2 \cdot f(GOP) \qquad (8)$$

where ω_{Rp} is the bitrate of P-frame when *GOP*=2 and M_L=1, and ω_2 is the weight for *f(GOP)*. To obtain the parameters for the *f(M$_L$)*, we applied least mean square approach using the normalized R_P of training video sequences when *GOP*=2. Also to estimate *f(GOP)*, we applied curve fitting approach on the *Rp* values of training video sequences at different *GOP* size settings, and found that $\omega_2\ln(GOP)$ provides a good estimate for *f(GOP)*. The value of ω_2 is estimated using least square regression from the training sequences. Assuming that the average bitrate of an I-frame is equal to R_I the average bitrate of a frame (R_f) is estimated as:

$$R_f = \frac{R_I}{GOP} + \omega_{RP} \cdot \left(0.92 + \frac{0.08}{(1+e^{3.56(6\cdot\delta_{CP}-0.84)})}\right) \cdot \frac{(GOP-1)}{GOP} \,. \qquad (9)$$
$$+ \omega_2 \cdot \ln(GOP) \cdot \frac{(GOP-1)}{GOP}$$

D. *Implementation of the Proposed Model*

To implement the proposed model, we need to obtain several variables from each video sequence. To this end, we encode the first two frames of each video sequence. Assuming that there is no scene change in the video sequence, the bitrate of each I-frame will be almost similar. Therefore, R_I is assumed to be equal to the bitrate of the encoded first frame while ω_{Rp} is equal to the bitrate of the second frame. For the complexity modeling, the *iprof* tool will provide us with the complexity of encoding the first two frames of the video sequence, i.e., $C_{2\text{-frames}}=C_I+Cp_{M_L=1}$. Since we already have the value of R_I from encoding the first two frames of each test sequence, we can estimate the value of C_I of these sequences. The value of $Cp_{M_L=1}$ can then be calculated using $C_{2\text{-frames}} - C_I$. Consequently, the value of ω_I is calculated using (2).

To estimate the modeling error, the average percentage of complexity and bitrate error for GOP={1, 2, 4, 8, 16, 32, 64} and M_L={1, 2, 3, 4, 5, 6, 7} is calculated. As Table III shows, the average error for complexity modeling is less than or equal to 3.45% for the test video sequences, while the average error of bitrate modeling is less than or equal to 11.6% as reported in Table IV.

TABLE III
COMPLEXITY MODELING ERROR

Video	Error (%)
RaceHorses	2.79
PeopleOnStreet	2.05
Vidyo1	3.45

TABLE IV
BITRATE MODELING ERROR

Video	Error (%)
RaceHorses	11.60
PeopleOnStreet	8.57
Vidyo1	9.55

III. ENCODING AND TRANSMISSION POWER CONSUMPTION MODEL

The total power dissipation at a sensor node consists of the power consumption for encoding (P_e), transmission (P_t) and reception (P_r). P_e can be calculated as follows:

$$P_e = C_f \cdot F_r \cdot CPI \cdot E_c \qquad (10)$$

where *CPI* is the number of CPU cycles to perform one basic instruction and E_c is the energy depletion per cycle. The transmission power consumption is calculated as:

$$P_t = \sum\left(\alpha + \beta \cdot d^{\eta}\right) \cdot R \qquad (11)$$

where α is a constant coefficient related to coding and modulation, β is the amplifier energy coefficient, *d* is the transmission distance, η is path loss exponent and *R* is the bitrate. The reception power consumption is calculated as:

$$P_r = \sum \lambda \cdot R \qquad (12)$$

TABLE V. PARAMETERS USED.

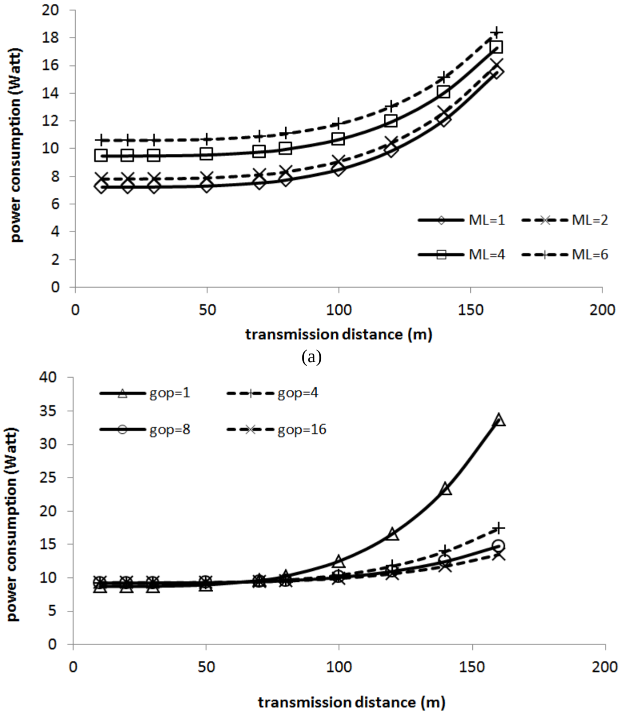
Parameters	Description	value
α	Energy cost for transmitting 1 bit	0.5 J/Mb
β	Transmit amplifier coefficient	1.3·10-8 J/Mb/m4
λ	Energy cost for receiving 1 bit	0.5 J/Mb
η	Path loss exponent	4
CPI	XScale average cycle per instruction [10]	1.78
E_c	Energy depleted per cycle for imote2 [6]	1.215 nJ

where λ is a constant coefficient representing energy cost for receiving 1 bit. Table V shows the parameters used for our experiments.

In this paper, we analyze a simple topology consisting of one video node and the sink. The total power consumption of a video node for different transmission distances for PeopleOnStreet video sequence is shown in Fig. 7. In this figure, we analyze two scenarios: a) the *GOP* size is fixed while the M_L varies, and b) the M_L is fixed while the *GOP* size changes. In Fig. 7a, the *GOP* size is set equal to eight and M_L changes. It is observed that for transmission distance less than 200m, the use of bigger M_L results in higher total power consumption. This result shows that varying M_L values do not significantly affect the trade-off between computation and communication. This trend is also seen in other test video sequences.

Fig. 7b shows the plot of total power consumption when M_L is equal to four and the *GOP* size changes. The figure shows that when the transmission distance is small, the configuration that leads to low power consumption is the one using smaller *GOP*. It means that the low encoding power consumption (due to the use of smaller *GOP*) is compensating the higher transmission power consumption (due to higher bitrate). However, when the transmission distance is large, the energy cost to transmit the data increased significantly. Therefore, we need to use the configuration with better compression performance, i.e., larger *GOP* size, to reduce the transmission energy consumption.

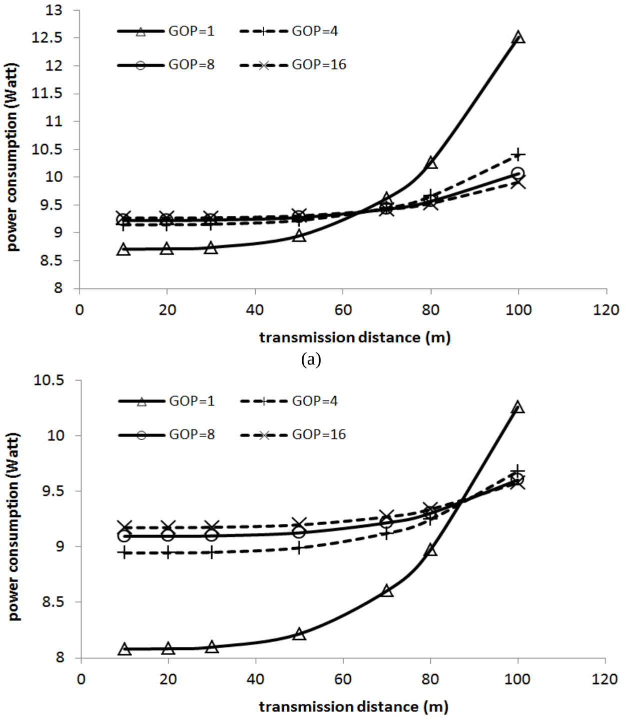
The trade-off between computation and communication can be clearly seen when the transmission distance is less than 100m as shown in Fig. 8. However, it can be seen that the transmission distance at which the use of bigger *GOP* minimizes power consumption is content dependent. For example, in the case of PeopleOnStreet video sequence, using *GOP* equal to one will minimize the total power consumption when the transmission distance is less than 63m (see Fig. 8a). However, for the RaceHorses video sequence, the use of *GOP* equal to one will minimize total power consumption when the transmission distance is less than 88m (see Fig. 8b).



(a)

(b)

Fig. 7. Total power consumption for different transmission distance: (a) *GOP*=8 and varying M_L (b) M_L=4 and varying *GOP* sizes



(a)

(b)

Fig. 8. Total power consumption for transmission distance less than 100m (M_L=4 and varying *GOP* sizes): (a) PeopleOnStreet sequence(b) RaceHorses sequence

IV. Conclusion

In this paper, we propose the encoding complexity and bitrate model of H.264-based video sensor networks. The experimental results show that the proposed complexity model provides a very small prediction error (less than or equal to 3.45%), while the bitrate modeling error is from 8.57% to 11.6% for the video sequences tested. The proposed model is used to show the trade-off between encoding and communication that can be exploited to minimize the total power consumption of VSNs.

Acknowledgment

This work was supported by the NPRP grant # NPRP 4-463-2-172 from the Qatar National Research Fund (a member of the Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, “A survey on wireless multimedia sensor networks,” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 51, no. 4, pp. 921–960, Mar. 2007.

[2] T. D. R¨aty, “Survey on Contemporary Remote Surveillance Systems for Public Safety,” Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol. 40, no. 5, pp. 493–515, Sep. 2010.

[3] I. E. Richardson, The H.264 Advanced Video Compression Standard, Second Edition. John Wiley & Sons, Ltd, 2010.

[4] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, “Overview of the H.264/AVC video coding standard,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 7, pp. 560–576, Jul. 2003.

[5] H. K. Zrida, A. C. Ammari, M. Abid, and A. Jemai, “Complexity/Performance Analysis of a H.264/AVC Video Encoder,” in Recent Advances on Video Coding, InTech.

[6] J. J. Ahmad, H. A. Khan, and S. A. Khayam, “Energy efficient video compression for wireless sensor networks,” presented at the Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on, Baltimore, MD, 2009, pp. 629 – 634.

[7] B. A. B. Sarif, M. T. Pourazad, P. Nasiopoulos, and V. C. M. Leung, “Encoding and communication energy consumption trade-off in H.264/AVC based video sensor network,” presented at the Accepted for publication IEEE World of Wireless, Mobile and Multimedia Networks, WoWMoM’13, 2013, pp. 1–6.

[8] P. M. Kuhn, “A Complexity Analysis Tool: iprof (version 0.41),” ISO/IEC JTC1/SC29/WG11/M3551, Jul-1998.

[9] ISO/IEC JTC1/SC29/WG11, “Joint Call for Proposals on Video Com-pression Technology.” Jan-2010.

[10] D. Chinnery and K. Keutzer, Closing the Power Gap between ASIC & Custom: Tools and Techniques for Low Power Design, 1st edition. Springer, 2007.

A Generalization of the PageRank Algorithm

Z. Bahrami Bidoni, R. George, K.A. Shujaee
Department of Computer and Information Systems
Clark Atlanta University
Atlanta, GA
{zeynab.bahrami, rgeorge, kshujaee}@cau.edu

Abstract— **PageRank is a well-known algorithm that has been used to understand the structure of the Web. In its classical formulation the algorithm considers only forward looking paths in its analysis- a typical web scenario. We propose a generalization of the PageRank algorithm based on both out-links and in-links. This generalization enables the elimination network anomalies- and increases the applicability of the algorithm to an array of new applications in networked data. Through experimental results we illustrate that the proposed generalized PageRank minimizes the effect of network anomalies, and results in more realistic representation of the network.**

Keywords- Search Engine; PageRank; Web Structure; Web Mining; Spider-Trap; dead-end; Taxation;Web spamming.

I. INTRODUCTION

With the rapid growth of the Web, users can get easily lost in the massive, dynamic and mostly unstructured network topology. Finding users' needs and providing useful information are the primary goals of website owners. Web structure mining [1],[2],[3] is an approach used to categorize users and pages. It does so by analyzing the users' patterns of behavior, the content of the pages, and the order of the Uniform Resource Locator (URL) that tend to be accessed. In particular, Web structure mining plays an important role in guiding the users through the maze. The pages and hyperlinks of the World-Wide Web may be viewed as nodes and arcs in a directed graph. The problem is that this graph is massive, with more than a trillion nodes, several billion links, and growing exponentially with time. A classical approach used to characterize the structure of the Web graph through PageRank algorithm, which is the method of finding page importance.

The original PageRank algorithm [3],[4],[5] one of the most widely used structuring algorithms, states that a page has a high rank if the sum of the ranks of its backlinks is high. Google effectively applied the PageRank algorithm, to the Google search engine [4]. Xing and Ghorbani [6] enhanced the basic algorithm through a Weighted PageRank (WPR) algorithm, which assigns a larger rank values to the more important pages rather than dividing the rank value of a page evenly among its outgoing linked pages. Each outgoing link page gets a value proportional to its popularity (its number of in-links and out-links). Kleinberg [7] identifies two different forms of Web pages called hubs and authorities, which lead to the definition of an iterative algorithm called Hyperlink Induced Topic Search (HITS) [8].

Bidoki and Yazdani [9] proposed a novel recursive method based on reinforcement learning [10] that considers distance between pages as punishment, called "DistanceRank" to compute ranks of web pages in which the algorithm is less sensitive to the "rich-get-richer" problem [9],[11] and finds important pages faster than others. The DirichletRank algorithm has been proposed by X. Wang et al [12] to eliminate the zero-one gap problem found in the PageRank algorithm proposed by Brin and Page [4]. The zero-one gap problem occurs due to the ad hoc way of computing transition probabilities. They have also proved that this algorithm is more robust against several common link spams and is more stable under link perturbations. Singh and Kumar [13] provide a review and comparison of important PageRank based algorithms.

As search engines are used to find the way around the Web, there is an opportunity to fool search engines into leading people to particular page. This is the problem of web spamming [14], which is a method to maliciously induce bias to search engines so that certain target pages will be ranked much higher than they deserve. This leads to poor quality of search results and in turn reduces the trust in the search engine. Consequently, anti-spamming is a big challenge for all the search engines. Earlier Web spamming was done by adding a variety of query keywords on page contents regardless of their relevance. In link spamming [15], the spammers intentionally set up link structures, involving a lot of interconnected pages to boost the PageRank scores of a small number of target pages. This link spamming does not only increasing the rank gains, but also makes it harder to detect by the search engines. It is important to point out that link spamming is a special case of the spider-traps [16]. At the present time, the Taxation method [16] is the most significant way to diminish the influence of the spider-traps and dead-ends by teleporting the random surfer to a random page in each iteration.

This article has two main contributions: First, we present a generalized formulation of the PageRank algorithm based on transition probabilities, which takes both in-link and out-links of node and their influence rates into account in order to calculate PageRanks. This would permit the application of this approach to a wide variety of network problems that require consideration of the current state values (and PageRank) as a function of past state transitions. Second, we describe a novel approach of adding virtual edges to a graph that permits more realistic computations of PageRank,

ISBN: 978-1-61208-324-7

negating the effect of network anomalies such as spider-traps and dead-ends.

The paper is organized as follows. In Section 2, a brief background review of the basic concepts for computing PageRanks based on transition probabilities is presented and the problems related to network anomalies such as spider-traps and dead-ends together with their solution method based on Taxation is stated. In Section 3, we introduce the proposed general approach for determining PageRank. In Section 4, we apply our PageRank method to a typical graph with all types of possible structures and inter/ intra-correlations and compare our results with the baseline technique. In Section 5, we conclude by describing the contribution of our method and discuss its results.

II. Overview on the PageRank approach based on transition probabilities

PageRank is a function that assigns a real number to each page in the Web. We begin by defining the basic, idealized PageRank, and follow it by modifications that are necessary for dealing with some real-world problems concerning the structure of the Web. Imagine surfing the Web, going from page to page by randomly (random surfer) choosing an outgoing link from one page to get to the next. This can lead to dead-ends at pages with no outgoing links, or cycles around cliques of interconnected pages. This theoretical random walk is known as a Markov chain or Markov process [16],[17].

In general, we can define the transition matrix of the Web to describe what happens to random surfers after one step. This matrix *M* has *n* rows and columns, if there are *n* pages. The element m_{ij} in row *i* and column *j* has value *1/k* if page *j* has *k* arcs out, and one of them is to page *i*. Otherwise, $m_{ij} = 0$. The probability distribution for the location of a random surfer can be described by a column vector whose *j*th component is the probability that the surfer is at page *j*. This probability is the (idealized) PageRank function.

Suppose we start a random surfer at any of the *n* pages of the Web with equal probability. Then the initial vector v_0 will have *1/n* for each component. If *M* is the transition matrix of the Web, then after one step, the probability distribution of the surfer place will be Mv_0, after two steps it will become $M\left(Mv_0\right) = M^2 v_0$, and so on. In general, multiplying the initial vector v_0 by *M* a total of i times will give us the distribution of the surfer after i steps.

This sort of behavior is an example of a Markov processes. It is known that the distribution of the surfer approaches a limiting distribution *v* that satisfies $v = Mv$, provided two conditions are met:

1) The graph is strongly connected; that is, it is possible to get from any node to any other node.

2) There are no dead-ends: nodes that have no arcs out.

In fact, because *M* is stochastic, meaning that each of its columns adds up to 1, v is the principal eigenvector. Note also that, because *M* is stochastic, the eigenvalue associated with the principal eigenvector is 1.The principal eigenvector of *M* tells us where the surfer is most likely to be after infinite steps *i*. The intuition behind PageRank is that the more likely a surfer is to be at a page, the more important the page is. We can compute the principal eigenvector of *M* by starting with the initial vector v_0 and multiplying by *M* some number of times, until the vector we get shows little change at each round. In practice, for the Web itself, 50–75 iterations are sufficient to converge to within the error limits of double-precision arithmetic.

A. Structure of the Web

It would be nice if Web pages were strongly connected. However, it is not the case in practice. An early study of the Web found it to have the structure shown in Figure 1. There is a large strongly connected component (SCC), but there were several other portions that were almost as large [18].

- The **in-component**, consisting of pages that could reach the SCC by following links, but were not reachable from the SCC.
- The **out-component**, consisting of pages reachable from the SCC but unable to reach the SCC.
- **Tendrils**, which are of two types. Some tendrils consist of pages reachable from the in-component but not able to reach the in-component. The other tendrils can reach the out-component, but are not reachable from the out-component.

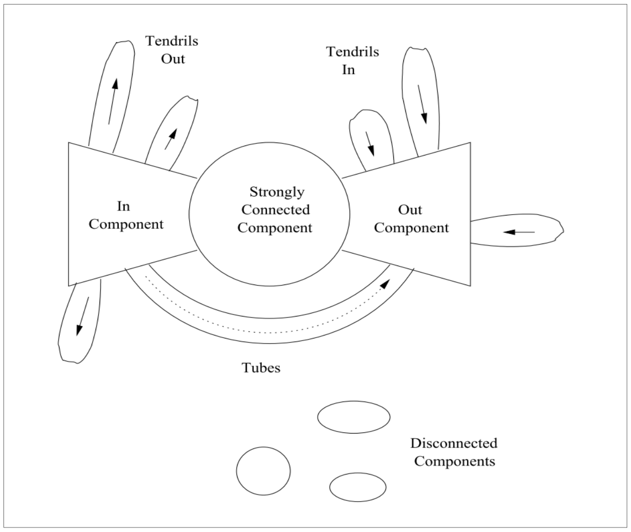


Figure 1. The “bowtie” representation of the Web [22]

In addition, there were small numbers of pages found either in

- Tubes, which are pages reachable from the in-component and able to reach the out-component, but unable to reach the SCC or be reached from the SCC.
- Isolated components that are unreachable from the large components (the SCC, in- and out-components) and unable to reach those components.

As a result, PageRank is usually modified to prevent such anomalies. There are, in principle, two problems we need to avoid. First, is the dead-end - a page that has no links out- which will bring a zero column in the forward transition matrix, and consequently it will cause all PageRanks to become zero. The second problem is groups of pages that all have out-links but they never link to any other pages. These structures are called spider-traps. Both these problems are solved by a method called "taxation," where we assume a random surfer has a finite probability of leaving the Web at any step, and new surfers are started at each page.

B. *Taxation*

To avoid the problem of spider-trap or dead-end, we modify the calculation of PageRank by allowing each random surfer a small probability of teleporting to a random page, rather than following an out-link from their current page. The iterative step, where we compute a new vector estimate of PageRanks v' from the current PageRank estimate v and the transition matrix M is

$$v' = \beta Mv + (1-\beta)e / n \tag{1}$$

Where β is a chosen constant, usually in the range 0.8 to 0.9, e is a vector of all 1's with the appropriate number of components, and n is the number of nodes in the Web graph. The term βMv represents the case where, with probability β, the random surfer decides to follow an out-link from their present page. The term $(1 - \beta)e/n$ is a vector each of whose components has value $(1-\beta)/n$ and represents the introduction, with probability $1 - \beta$, of a new random surfer at a random page.

Although by employing this formulation, the effect of spider-trap and dead-end is controlled and the PageRank is distributed to each of other nodes, components of spider-trap still are managed to get most of the PageRank for themselves. Therefore, the PageRanks of nodes are still unreasonable. For instance, in Figure 2. , C is a simple spider trap of one node and the transition matrix is as follows:

$$M = \begin{bmatrix} 0 & 1/2 & 0 & 0 \\ 1/3 & 0 & 0 & 1/2 \\ 1/3 & 0 & 1 & 1/2 \\ 1/3 & 1/2 & 0 & 0 \end{bmatrix} \tag{2}$$

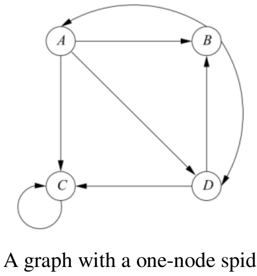


Figure 2. A graph with a one-node spider trap

If we perform the usual iteration to compute the PageRank of the nodes, we get

$$\begin{bmatrix} 1/4 \\ 1/4 \\ 1/4 \\ 1/4 \end{bmatrix} \begin{bmatrix} 3/24 \\ 5/24 \\ 11/24 \\ 5/24 \end{bmatrix} \begin{bmatrix} 5/48 \\ 7/48 \\ 29/48 \\ 7/48 \end{bmatrix} \begin{bmatrix} 21/288 \\ 31/288 \\ 205/288 \\ 31/288 \end{bmatrix} \cdots \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \tag{3}$$

As predicted, all the PageRank is at C, since once there a random surfer can never leave. To avoid the problem illustrated, we modify the calculation of PageRank by the Taxation method. Thus, the equation for the iteration becomes

$$\mathbf{v}' = \begin{bmatrix} 0 & 2/5 & 0 & 0 \\ 4/15 & 0 & 0 & 2/5 \\ 4/15 & 0 & 4/5 & 2/5 \\ 4/15 & 2/5 & 0 & 0 \end{bmatrix} \mathbf{v} + \begin{bmatrix} 1/20 \\ 1/20 \\ 1/20 \\ 1/20 \end{bmatrix} \tag{4}$$

Notice that we have incorporated the factor β into M by multiplying each of its elements by $4/5$. The components of the vector $(1 - \beta)e/n$ are each $1/20$, since $1 - \beta = 1/5$ and $n= 4$. The first iteration:

$$\begin{bmatrix} 1/4 \\ 1/4 \\ 1/4 \\ 1/4 \end{bmatrix} \begin{bmatrix} 9/60 \\ 13/60 \\ 25/60 \\ 13/60 \end{bmatrix} \begin{bmatrix} 41/300 \\ 53/300 \\ 153/300 \\ 53/300 \end{bmatrix} \begin{bmatrix} 543/4500 \\ 707/4500 \\ 2543/4500 \\ 707/4500 \end{bmatrix} \cdots \begin{bmatrix} 15/148 \\ 19/148 \\ 95/148 \\ 19/148 \end{bmatrix} \tag{5}$$

By being a spider trap, C has still managed to get more than half of the PageRank for itself. However, the effect has been limited, and each of the nodes gets some of the PageRank.

III. A GENERALIZED METHOD

In web arena, a link by important pages will impact on significance of a page. However, there are other networks in which not just in-link but out-links are also weighty. For instance, in social networks, connecting to eminent people (out-link) is as crucial as being connected by key persons (in-link) in evaluating the degree of prominence of a member. Therefore, sometimes sorting and grading nodes of a graph only based on in-links will result in an incorrect evaluation. So, we take out-links and the rate of their impacts with respect to in-links into our computations.

A. *Algorithm*

Suppose we start as a random surfer at any of the n pages of the Web with equal probability. Then the initial vector will have $1/n$ for each component. If M_f is the forward transition matrix of the Web, then after one forward step, the probability distribution of the next surfer place will be $M_f v_0$ and if M_b is the backward transition matrix of the Web, then after one backward step, the probability distribution of the previous surfer place will became $M_b v_0$. Also, we consider the importance weight factor of both in-links (β) and out-links ($1-\beta$).

Note that equation $\left(\beta M_f + (1-\beta) M_b\right)$ is the linear combination of both next and previous surfer place, and it is also stochastic because it is a linear combination of two stochastic matrices. So its eigenvalue associated with the principal eigenvector will be 1. The principal eigenvector of $\left(\beta M_f + (1-\beta) M_b\right)$ tells us where the surfer is most likely to be after a long time. Recall that the intuition behind PageRank is that the more likely a surfer is to be at a page, the more important the page is. We can compute the principal eigenvector of $\left(\beta M_f + (1-\beta) M_b\right)$ by starting with the initial vector v_0 and multiplying by $\left(\beta M_f + (1-\beta) M_b\right)$ some number of times, until the vector we get shows little change at each round. Considering this matrix instead of M_f has two advantages: First, in computing PageRank of a node, the importance of its neighbors with both types of relationship (out-link and in-link) and their arbitrary impact rates (parameter β) have taken into account. Second, by using this method, we do not have the problems about dead-ends and spider-traps because we take the linear combination of entering probability from and exiting probability to other nodes in our computation. Therefore, in case $\beta \neq 0$ and $\beta \neq 1$, the columns related to dead-ends are not completely zero. Likewise, for the spider-trap columns, probabilities related to other nodes are not zero and they cannot absorb more unreasonable rank to themselves. About cases $\beta = 1$ or $\beta = 0$, in the following, we proposed another idea (adding virtual edges) by which the random surfer can exit from dead-ends and spider-traps.

The proposed algorithm is as follows:

Step 1: finding Forward and Backward transition matrices.

Step 2: considering appropriate formula and keep iterating until it gets converged.

In this step, three possible conditions can exist which are characterized as following:

Case 1: $\beta \neq 0$ **and** $\beta \neq 1$**.** It means that both forward and backward trends are important to calculate PageRanks. Thus, we only need to calculate the eigenvector of matrix $\left(\beta M_f + (1-\beta) M_b\right)$.

Case 2: $\beta = 1$ So, we need only the forward matrix to calculate PageRanks. If there are not a dead-end or a spider-trap in the graph, the vector of PageRanks is the eigenvector of M_f . If there are dead-ends or spider-traps, the eigenvector of M_f assigns most of PageRank to spider-traps and dead-ends that is not real. Thus we add enough virtual out-links to remove these spider and dead-end situations. For each dead-end and spider-trap, we will consider a virtual edge in which source of them are dead-ends and one member of each spider-traps, respectively. Also, their destinations can be any arbitrary nodes, excepting those of dead-end and spider-traps (see Figure 3. Green color edges). Hence, If assumed v is eigenvector of matrix $M_f^{'}$ (forward transition matrix after adding virtual links), in order to find final PageRanks of vertices, we have to remove effect of these virtual links on PageRanks by calculating the following equation $v - (M_f^{'} - M_f)v$.

Case 3: $\beta = 0$. Here only backward trend (out-links) is important to consider for calculation of PageRanks. So we only need backward matrix to determine PageRanks. If there are not in-component or in-tendril vertices in the graph, vector of PageRanks is eigenvector of M_b. If there are in-component or in-tendril vertices, eigenvector of M_b assigns most of PageRank to in-component and in-tendril vertices, which is not real. Thus we add enough virtual in-links to remove these in-component and in-tendril situations then after computing eigenvector of new backward matrix $M_b^{'}$, we have to remove effect of these virtual links on PageRanks (see Figure 3. Red color edges). If suppose v is eigenvector of matrix $M_b^{'}$(backward transition matrix after adding virtual links). The final PageRanks of vertices would be $v - (M_b^{'} - M_b)v$.

Step 3: normalize PageRank vector to find distribution probability of vertices.

As shown below, if we consider a matrix include the importance of pairwise comparison of vertices (A), eigenvector of this matrix would be distribution probability of vertices.

Note that, W is vector distribution probability of vertices that sum of its components is 1 and also w_i is amount of vertex i‘s importance. So, instead of w_i / w_j in matrix A, we let p_i / p_j , which p_i , p_j are PageRanks of nodes i, j. We calculate eigenvector of matrix A and to get the distribution probability of vertices.

$$AW = \begin{bmatrix} w_1/w_1 & w_1/w_2 & \cdots & w_1/w_n \\ w_2/w_1 & w_2/w_2 & \cdots & w_2/w_n \\ \vdots & \vdots & \cdots & \vdots \\ w_n/w_1 & w_n/w_2 & \cdots & w_n/w_n \end{bmatrix} * \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = n * \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = nW \qquad (6)$$

B. *Biased Random Walk*

In order to bias the rank of all nodes with respect to a special subset of nodes, we use the Biased Random Walk method in which the random surfer, in each iteration, will jump on one of the member of the subset with equal probability. Its most important application is topic-sensitive PageRank [19] in search engines. The consequence of this approach is that random surfers are likely to be at an identified page, or a page reachable along a short path from one of these known pages, because the pages they link to are also likely to be about the same topic. The mathematical formulation for the iteration that yields topic-sensitive PageRank is similar to the equation we used for general PageRank. The only difference is how we add the new surfers. Suppose S is a set of integers consisting of the row/column numbers for the pages we have identified as belonging to a certain topic (called the teleport set). Let e_s be a vector that has 1 in the components in S and 0 in other components. Then the topic-sensitive PageRank for S is the limit of the iteration

$$v' = \alpha(\beta M_f + (1-\beta)M_b)v + (1-\alpha)e_s / |s|$$
$$0.8 \le \alpha \le o.9 \qquad (7)$$

Here, as usual, M is the transition matrix of the Web, and $|S|$ is the size of set S.

IV. THE EXPERIMENT

Figure 3. is a graph with 20 vertices that include all kinds of network artifacts mentioned in section 2.

SCC:{1,2,4,5,7,8,9,10,15,17,18,20} TUBE:{16-6}

OUT-COMPONENT:{6,11,12} IN-COMPONENT:{3,13,16}
OUT-TENDRIL:{14} IN-TENDRIL:{19}

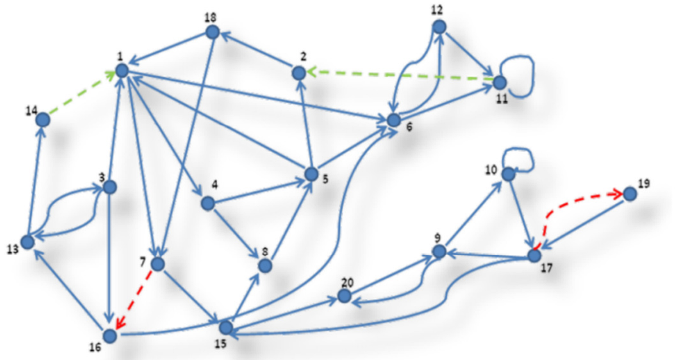


Figure 3. Synthetic Graph Example

In case 2 ($\beta = 1$), there are a dead-end situation on vertex 14 and a spider-trap situation on set of vertices {6, 11, 12}, and in order to remove the dead-end and the spider-trap consider 2 virtual out-link (green edges) on these vertices. Also in case 3 ($\beta = 0$), there are in-component situation on set of vertices {3, 13, 16}, and in order to remove negative PageRank consider 2 virtual in-link (red edges) on these vertices. For completeness, we also compute the biased random walk on case1. Comparing the results with case1, TABLE I. , it is clear that PageRanks are biased on set S={2, 4, 7, 18}. As we expect, rank of nodes of set S and nodes that are pointed by set S get higher ranks.

TABLE I. PAGERANK VECTOR AT CASES 1, 3, AND BIASED RANDOM WALK.

Results of case 1 ($\beta = 0.7$)		Results of the biased random walk on case1		Results of case 3 ($\beta = 0$)	
Nodes number	***PageRank***	***Nodes number***	***PageRank***	***Nodes number***	***PageRank***
11	0.945	5	0.9937	17	0.57916
12	0.2177	11	0.9878	10	0.38611
6	0.1767	18	0.9703	13	0.36037
9	0.0703	1	0.9432	1	0.27028
10	0.0632	7	0.9013	3	0.27028
5	0.0601	15	0.8513	5	0.25741
1	0.0543	2	0.7444	9	0.25741
20	0.0527	4	0.6847	7	0.24454
15	0.0495	6	0.65	4	0.19305
17	0.045	8	0.6414	19	0.19305
8	0.036	9	0.5045	16	0.18018
7	0.029	20	0.4878	2	0.16731
4	0.0272	12	0.3659	18	0.16731
18	0.025	10	0.3204	8	0.1287
3	0.0237	17	0.2976	15	0.1287
13	0.023	3	0.1628	20	0.1287
16	0.0223	13	0.1144	12	1.14E-17
2	0.0216	16	0.0923	6	7.34E-18
14	0.0081	19	0.0386	11	0
19	0.0068	14	0.035	14	0

TABLE II. COMPARING RESULTS OF THE ALGORITHM AND TAXATION METHOD TO AVOID ANOMALIES IN CASE 2 ($\beta = 1$)

Using virtual edges		Taxation	
nodes no	***PageRank***	***nodes no***	***PageRank***
9	0.508068237	11	0.83086
10	0.508068237	9	0.25352
20	0.381051178	10	0.22903
2	0.265581124	20	0.19944
17	0.254034118	15	0.15968
15	0.254034118	6	0.1495
5	0.173205081	5	0.14569
18	0.161658075	17	0.14155
8	0.15011107	8	0.11547
1	0.138564065	1	0.11197
6	0.138564065	7	0.08907
7	0.127017059	12	0.08748
11	0.103923048	18	0.07921
12	0.069282032	2	0.06521
4	0.046188022	4	0.05567
3	7.50E-17	13	0.0528
13	2.12E-17	3	0.04612
16	1.16E-17	14	0.04612
14	1.02E-17	16	0.0369
19	0	19	0.02386

Comparing the results of the Taxation method and our proposed method, TABLE II. , obviously we can realize that our approach produces more reasonable outcomes. Because, as it is shown in the TABLE II, node 9 is the junction of two cycles, all nodes of these cycles are from SCC part of the graph, so the random surfer is most likely on it. The nodes 10 and 20 have higher rank after 9, because they have in-link from the node 9. The rank of node 5 cannot be higher than 17 because the node 17 is a member of the cycle consist of node 9 and 10. In Taxation result, the nodes with spider-trap situation such as 6 and 11 got higher and vertices 2 and 18 got lower PageRank than our proposed approach results. Also, for other vertices, their ranks are either the same or very close to each other's.

V. CONCLUSION

In this paper, the fundamental idea of Web Structure mining and Web Graph is explained in detail to have a generic understanding of the data structure used in web. The main purpose of this paper is to present the new PageRank based algorithms and compare that with the previous algorithms.

The proposed method generalizes the approach of finding PageRank based on transition probabilities by considering the arbitrary impact rates of both out-links and in-links, in order to include all possible cases because there are some conditions in which out-links have also an influence on PageRank of nodes. Moreover, it prevents that spider-traps and dead-ends have a high unreasonable rank and assign higher PageRanks to themselves. The noticeable weak point of previous method is that it assigns more unreasonable PageRank to spider-traps and dead-ends, and also reduces PageRank of SCC vertices. But in our approach this problem has been solved, because by adding virtual edges, random surfers will not stop on spider-traps and dead-ends. According to [13], DirichletRank has been so far the best method amongst previous methods, capable of diminishing the impact of link spamming (a special case of spider-traps) and dead-end problem that is, however, only applicable to backward analysis. Our approach in comparison with their method is general for more types of networks and simpler to understand and implement. Also, by using ideas suggested in this paper, in any possible cases, PageRanks is insulated from the influence of anomalies including in/out-tendrils and in/out-components.

The generalization of the PageRank algorithm to include forward and backward links into a node makes this approach applicable to new domains beyond web mining and search engines. We are currently exploring the application of the new generalized algorithm to the analysis of network data for instance using PageRank as a measurement of node's activity score [20] to find communities.

ACKNOWLEDGMENT

This research is funded in part by the Army Research Laboratory under Grant No: W911NF-12-2-0067 and Army Research Office under Grant Number W911NF-11-1-0168. Any opinions, findings, conclusions or recommendations expressed here are those of the author(s) and do not necessarily reflect the views of the sponsor.

+

REFERENCES

[1] R. Kosala and H. Blockeel, “Web mining research: A survey,” ACM SIGKDD Explorations, 2(1), 2000, pp. 1–15.

[2] S. Madria, S. S. Bhowmick, W. K. Ng, and E.-P. Lim, “Research issues in web data mining,” In Proceedings of the Conference on Data Warehousing and Knowledge Discovery, 1999, pp. 303–319.

[3] S. Pal, V. Talwar, and P. Mitra, “Web mining in soft computing framework : Relevance, state of the art and future directions,” IEEE Trans. Neural Networks, 13(5), 2002, pp. 1163–1177.

[4] L. Page, S. Brin, R. Motwani, and T. Winograd, “The PageRank citation ranking: Bringing order to the web,” Technical report,Stanford Digital Libraries SIDL-WP-1999-0120, 1999.

[5] C. Ridings and M. Shishigin, “Pagerank uncovered,” Technical report, 2002.

[6] W. Xing and A. Ghorbani, “Weighted PageRank Algorithm,” Proc. of the Second Annual Conference on Communication Networks and Services Research (CNSR ’04) IEEE, 2004 , pp. 305-314, 0-7695-2096-0/04 .

[7] J. Kleinberg, “Authoritative Sources in a Hyper-Linked Environment”, Journal of the ACM 46(5), 1999, pp. 604-632.

[8] S. Chakrabarti, et al. "Mining the Web's link structure." Computer 32.8 ,1999, pp. 60-67.

[9] A. M. Zareh Bidoki and N. Yazdani, “DistanceRank: An intelligent ranking algorithm for web pages,” Information Processing and Management, Vol 44, No. 2, 2008, pp. 877-892.

[10] R.S. Sutton and A.G. Barto, “Reinforcement Learning: An Introduction,” Cambridge, MA: MIT Press, 1998.

[11] J. Cho, S. Roy and R. E. Adams, “Page Quality: In search of an unbiased web ranking,” Proc. of ACM International Conference on Management of Data,”. 2005, pp. 551-562.

[12] X. Wang, T. Tao, J. T. Sun, A. Shakery, and C. Zhai, “DirichletRank: Solving the Zero-One Gap Problem of PageRank,” ACM Transaction on Information Systems, Vol. 26, Issue 2, 2008.

[13] A. K. Singh and P. Ravi Kumar. "A Comparative Study of Page Ranking Algorithms for Information Retrieval," International Journal of Electrical and Computer Engineering 4, no. 7 (2009), pp. 469-480.

[14] Z. Gyongyi and H. Garcia-Molina, “Web Spam Taxonomy,” First International Workshop on Adversarial Information Retrieval on the Web *(AIRWeb 2005)*, 2005.

[15] Z..Gyongyi and H. Garcia-Molina, “Link Spam Alliances,” Proc. of the 31st International Conference on Very Large DataBases (VLDB), 2005, pp. 517-528.

[16] A. Rajaraman, J. Leskovec, and J. D. Ullman, “Mining of Massive Datasets,” 2013, pp.161-198.

[17] S. Brin and L. Page, “Anatomy of a large-scale hypertextual web search engine,” Proc. 7th Intl. World-Wide-Web Conference, 1998, pp. 107–117.

[18] A. Broder, et al. "Graph structure in the web," *Computer networks* 33.1 , 2000, pp. 309-320.

[19] T.H. Haveliwala, “Topic-sensitive PageRank,” Proc. 11th Intl. World-Wide-Web Conference, 2002, pp. 517–526.

[20] J. Qiu and Z. Lin, “A framework for exploring organizational structure in dynamic social networks,” Decision Support Systems, 51, 2011, pp.760–771.

PROLOG: Evaluating Attentional Capacity in Special Working Centers

Kinect technology tasks for cognitive assessment of disabled workers

Anna Vilaro and Pilar Orero

Catalan Centre for Research in Ambient Intelligence and Accessibility, CAIAC
Autonomous University of Barcelona, UAB
Barcelona, Spain
anna.vilaro@uab.cat, pilar.orero@uab.cat

***Abstract*—The PROLOG project aims to provide a complementary tool for the assessment of cognitive skills of mentally disabled working people. The project provides a platform to evaluate, in a quick and personalized way, the attentional performance of users through specific tasks. Interaction with the tests is done by Kinect technology. The platform records the worker's performance on various tasks and presents the evolution over time in order to detect possible cognitive impairment. Longitudinal evaluation of cognitive impaired workers will help the existing unbalanced retirement practices.**

Keywords: cognitive impairment; evaluation; attention; Kinect.

I. Introduction

Elder mentally disabled people may suffer cognitive impairment associated with premature ageing. This impairment is usually related to difficulties in maintaining attention and problems associated with memory, plus many other physical related challenges.

The employment of cognitive impaired people -or mental illness- is a social objective that contributes to improve the quality of life of cognitive impaired workers, providing many benefits such as a full social integration [3]. The deterioration of these basic cognitive abilities may hinder the performance of job duties or even stay in employment. For example, the inability to maintain sustained attention (concentration) can hamper the worker to complete the tasks or steps in a process; or problems with memory may make it difficult to remember already learned tasks or learn new ones. Thus, there is a need to have a longitudinal assessment throughout the working life of these workers in order to ensure that the employee retains the skills that were described in the initial evaluation. Thus, tools to help assess the degree of disability and the development of the individual throughout his/her working history are required to optimize the evaluation process.

The PROLOG project aims to provide a complementary tool for the assessment of cognitive skills of mentally disabled working people. The project develops an Information and Communication Technologies tool with a set of tests to assess cognitive impairment of people with intellectual disabilities working in special employment centres. PROLOG has its innovation in incorporating Kinect technology [6] that recognizes body movements and voice to interact with applications. This technology, as applied to the field of rehabilitation of disabled people, is being used for the first time to develop tests to assess attentional capacity.

Currently, the tests used to assess attentional capacity are not adapted for people with cognitive impairments. Furthermore, the tests use to be paper-based and need to be carried out by a specialist, taking considerable administration.

The project presents three important improvements regarding the current evaluation tools: 1) Creation of new interaction of existing attentional tests which are already in use for evaluation of workers with cognitive disabilities; 2) Creation of evaluation benchmarking to correlate the results of attentional tests. Values will be objective and numeric, allowing a longitudinal evaluation across the working life of the person; and 3) Creation of personalised exercises, complementary with tests, to exercise attention and maintain skills. Also, the user-centric approach of the project contributes to an added value, since it makes the application friendly for any group of users.

In the following Methodology section, the content of the tests is presented. Then, the paper outlines the contribution of the project as well as future work.

II. Methodology

In this first stage of the project, we designed a series of new tests based on validated psychological tests. Specifically, attentional capacity was chosen because it is a fundamental cognitive function that is usually seen rapidly affected in the presence of cognitive impairment, making it difficult for other executive functions to take place. The project also provides a platform to record the execution of various tasks and users and their carers can see the evolution over time in order to detect possible cognitive impairment.

Currently, the tests are being implemented and we expect to have a preliminary version of the tests ready for pilot testing by February 2014.

We aim to create attractive and motivating tasks, using similar stimuli and goals presented in videogames. During the first year, three tests are being designed to evaluate different dimensions of attention. Specifically, the tests aim to evaluate sustained attention (two tests) and selective attention (one test). The design of such tests is presented below.

A. Evaluating sustained attention

Sustained attention can be defined as the ability to maintain attention during continuous and repetitive activity.

We designed two tests aimed at assessing the ability to sustain attention over a period of time.

We adapted the test Sustained Attention to Response Task, SART [2][4]. This test aimed at measuring the ability of a person to inhibit responses to infrequent and unpredictable stimuli during a period of rhythmic and rapid responses to a frequent stimuli (generally associated with the detection of an unlikely-to-occur stimuli). SART test presents only one digit at a time, and the participant's task is to quickly respond to all numbers except to one in particular (e.g., touching the screen in every trial, except when the number 3 is presented). Thus, it is a reaction time task that evaluates sustained attention through an element of response suppression.

In our test adaptation, we replaced the digits for images (insects, for example) in order to make it more attractive to users. The goal of the game would be to hunt insects in a forest with a network hunt. During the test, images of insects appear rhythmically in various predetermined positions of the screen. Similar to SART test, the task is to "catch" all the insects, except one in particular. The user has to perform a motor response (i.e. raise the hand simulating the action of grasping) when the stimuli is detected, or do nothing when appropriate. Thus, the user has to pay attention to avoid hunting a pre-defined insect or element. The test finishes when the participant exceeds a determined number of errors, or when a time limit is over. After the test, performance results are presented such as for how long the test lasted or the number of errors during a predefined interval of time.

In a second task, we adapted the TAP test [5]. This task requires the comparison of two subsequent stimuli in order to determine if these two stimuli have a predetermined feature in common. This procedure requires the use of working memory and flexibility and, in a more complex variant, the ability to divide attention, as two aspects of the stimulus must be taken into account.

In our adaptation for Kinect, users ware presented with a background image (e.g., a forest) with some highlighted regions where the stimuli may appear. Following the example of the insects, the user's task is to detect as quickly as possible whether the stimulus is the same as before (e.g., same insect), or not. Thus, there are two possible answers (same or different) that the user perform raising right or left hand in order to activate buttons showed in the screen. When the tests finishes, results such as the percentage of correct answers, errors and omissions, as well as reaction time are presented.

B. *Evaluating selective attention*

Selective attention is the ability to attend one or two important stimuli, while deliberately suppressing the consciousness of the distracting stimuli. In order to assess selective attention, we adapted the Flanker Compatibility Effect [1]. This is an experimental task designed to study factors that may affect selective attention, and to what extent information processing of irrelevant information occurs. The experimental task is to attend a central stimulus flanked by other stimuli called flanks or distracters. The subject's task is to identify the central stimulus (for example, a letter) and ignore the side letters.

In our adaptation of the test, the stimuli are images of insects that point to a particular direction (for example, images of three caterpillars pointing to the left). User task's is to say whether the central insect looks to the left or right (caterpillars presented on the sides can point to the same direction or the opposite). The user must indicate if the direction of the track is to the right or left. At the end of the test, performance results would inform about percentages of correct responses, errors and omissions, as well as the average reaction time.

In all tests, the results can be displayed for a particular session, or in graphical comparisons between multiple sessions (of the same or different users). Also, given the user centric approach of the application, the test parameters can be modified through a configuration screen before starting, and these parameters can be saved for each user in the platform in order to adapt the difficulty of the tests to different users. For example, it may offer the possibility to choose a category of stimuli (fruits, colours, shapes, etc.), or to define which particular element is defined as target stimulus within a category. Additionally, other parameters may be configured such as presentation time of the stimuli, the duration of the interval between stimuli, or the number of trials in each test.

In the final phase of the project, we will conduct a validation test. In this sense, the tests will be carried out to employees of several special working centres in Catalonia. Two groups will be defined in order to compare tests results, one group showing signs of cognitive impairment or not. To verify the concurrent validity of the tests, the results of both groups will be compared with other existing assessments (e.g., ICAP test, medical evaluations, etc.), and potentially affecting variables will be controlled.

III. CONTRIBUTION

The PROLOG assessment tool will have an important impact. Health and safety risks will be monitored, and, when an employee is no longer able to work, it will be possible to show the progression in the deterioration, avoiding the existing reality of disabled workers having to work until the retirement age of 67, unable to perform any task, still having to go to work every day.

IV. CONCLUSION AND FUTURE WORK

The implementation of the evaluation tool, together with the platform to manage will allow working special centres to assess their employees and detect and confirm possible cognitive impairments. Despite the fact that the project it is in its first version, the usefulness of the tool had been appreciated by the psychologists from the special working centres. The first preliminary tests showed the value of the tasks as a complementary assessing tool as well as an engaging way of training attentional skills.

In the future, it is planned to extend the number of tests to assess other cognitive skills such as memory or executive functions. Also, new exercises with Kinect will be created as training sessions to improve or maintain cognitive abilities.

Regarding the platform, it is expected to provide support for a possible protocol to evaluate the continuity on the workplace, containing extra information from other medical and neuropsychological tests. Thus, the evaluation tool would be useful to the users themselves (to see their evolution), the company-employer, and finally the government.

ACKNOWLEDGMENT

The PROLOG project is being developed by the Centre d'Accessibilitat i Intel·ligència Ambiental de Catalunya (CAIAC), together with Indra, Adecco Foundation, PRODIS and UAB, and is part of the Cátedra INDRA de Tecnologías Accesibles.

REFERENCES

[1] B. A. Eriksen and C. W. Eriksen, “Effects of noise letters upon the identification of a target letter in a nonsearch task”, Perception and Psychophysics, vol. 16(1), pp. 143-149, 1974.

[2] T. Manly, I. H. Robertson, M. Galloway and K. Hawkins, “The absent mind: further investigations of sustained attention to response”, Neuropsychologia, vol. 37(6), pp. 661-70, 1999.

[3] M. Paredes Gascón, M. Fernández-Cid Enríquez and M. J. Ruiz Figueroa, “Prevención de riesgos laborales entre las personas con discapacidad intelectual en los centros especiales de empleo”, Cuadernos de Trabajo Social, 25 (1), pp. 249-260, 2012.

[4] I. H. Robertson, Manly, T., J. Andrade, B.T. Baddeley and J. Yiend, “‘Oops!’: performance correlates of every-day attentional failures in traumatic brain injured and normal subjects”, Neuropsychologia, vol. 35(6), pp: 747-758, 1997.

[5] P. Zimmermann, M. Gondan, and B. Fimm (2002). KITAP, Testbatterie zur Aufmerksamkeitsprüfung für Kinder [Attention test battery for children]. Herzogenrath, Germany: Vera Fimm, Psychologische Testsysteme.

[6] Z. Zhang, “Microsoft Kinect Sensor and Its Effect”, Multimedia at work. IEEE multimedia, pp. 4-10, April 2012.

Detection of Persuasion Campaigns on Twitter™ by SAX-VSM Technology

Sergey Malinchik
Lockheed Martin Advanced Technology Laboratories
Cherry Hill, NJ 08002, USA
sergey.b.malinchik@lmco.com

Abstract— **In this paper, we present a novel approach for detection of persuasion campaigns in online social networks. We demonstrate that temporal evolution of different information cascades in social media display unique signatures of diffusion patterns which are indicators of different kinds of information spreads in underlying networks. We describe a progress of information diffusion through networks by multidimensional time series, representing temporal behavior of multiple cascade features and apply our SAX-VSM technique for classification of the time series. This approach allows us to distinguish two types of topics on Twitter™, promoted or advertisement campaigns and non-promoted or naturally trending topics. We show that the classification can be done without content analysis of topics, using only network topological features, statistics of users' temporal activity within networks, and some metadata. Optimal selection of right information cascade features allows to achieve classification accuracy ~ 97%.**

Keywords – Twitter™; advertisement; persuasion detection

I. INTRODUCTION

Currently, more and more individuals are involved in social media activities, and the opinions of millions of people are significantly formed under the influence of information spread through social networks [1], [2], [3]. It is not surprising that the number of attempts trying to organize influencing campaigns is growing [4], [5], [6], [7]. Persuasion campaigns are targeting wide audience and deliver topics with special vision aimed at shifting beliefs and opinions of participants.

Meme tracking, text mining and sentiment analysis tools become more powerful, but these tools perform only the easiest portions of the analysis process and are unable to distinguish between natural and artificially generated conversations, or between process of normal opinion exchange and invisible orchestrated work of influence. These tools will likely miss emerging persuasion campaigns.

New efficient and effective techniques that facilitate to process in real time, large data streams and detect organized influencing in social media are in high demand.

We present a new way of detecting persuasion campaigns by training a system to learn signatures of temporal evolution patterns of information cascades and perform detection at high accuracy without sophisticated content analysis.

The paper is structured as follows: Section II provides background for our main hypothesis and SAX-VSM technique; Section III gives a short description of data acquisition and presents classification experiments; Section IV discusses relevant work, and, in Section V, we conclude and discuss future work.

II. BACKGROUND

A. Concept and Approach

Our main hypothesis is that the detection of orchestrated persuasion and deception campaigns in social media can be done by monitoring temporal behavior of information cascades and analyzing patterns of their time-evolution (see Figure 1).

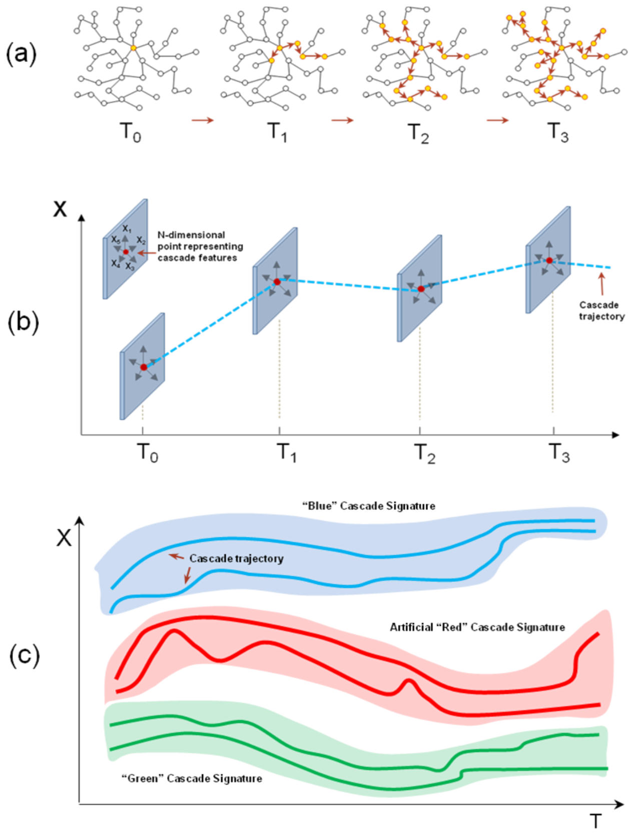

(a)
T0
T1
T2
T3
(b)
X
X1
X2
X3
X4
X5
N-dimensional point representing cascade features
Cascade trajectory
T0
T1
T2
T3
(c)
X
"Blue" Cascade Signature
Cascade trajectory
Artificial "Red" Cascade Signature
"Green" Cascade Signature
T

Figure 1. Illustartion of the "cascade signature" concept.

Our approach can be formulated as follows:

i. At each time step of the information cascade evolution, by measuring the multiple features of the underlying communication network, we represent the cascade at a given moment in time as a feature vector (point) in the multi-dimensional feature space (see Figures 1a and 1b).

ii. By tracking the cascade feature vector, we monitor the evolution of cascade as a multi-dimensional time series or *cascade trajectory*.

iii. We assume that cascade trajectories (multi-dimensional time series) can represent the different classes of conversation patterns or *cascade signatures* (see Figure 1c) that occur in online social media.

B. *SAX-VSM Classification Algorithm*

Recently, we proposed a novel method for temporal data analysis and classification, called SAX-VSM [8], which is based on two existing techniques namely, SAX (Symbolic Aggregate approXimation) [9] and VSM (Vector Space Model) [11]. The SAX-VSM algorithm demonstrates a high accuracy performance, learns efficiently from a small training set, and has a low computational complexity.

The first component of SAX-VSM is Symbolic Aggregate Approximation (SAX). The basic idea of SAX [9], [10], is to convert data into a discrete format, with a small alphabet size. To convert a time series into symbols, it is first z-normalized, and two steps of discretization are performed. First, a time series is transformed using Piecewise Aggregate Approximation (PAA). PAA approximates a time series by dividing it into equal-length segments and recording the mean value of the data points that fall within the segment. Next, to convert the PAA values to symbols, a user determines the breakpoints that divide the distribution space into $N_{alphabet}$ equiprobable regions, where the alphabet size, $N_{alphabet,}$ is specified by the user. The PAA coefficients can then be easily mapped to the symbols corresponding to the regions in which they reside. Fig. 2 shows an example of a time series being converted to string *baabccbc*. It was shown that the general shape of the time series is still preserved, in spite of the enormous dimensionality reduction.

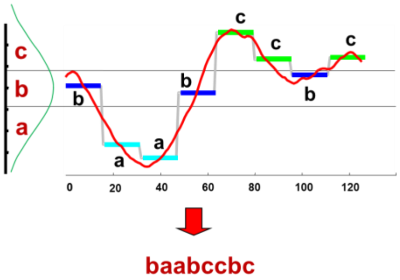


Figure 2. Visualization of the SAX dimensionality reduction technique (adopted from [9]). A time series (red line) is discretized thirst by a PAA procedure (N_{PAA} = 8) and then using predetermined breakpoints is mapped into the word "baabccbc" using an alphabet size of 3 ($N_{alphabet}$ = 3).

The second component of SAX-VSM technique is a well-known in Information Retrieval a Vector Space Model, VSM [11]. In order to build SAX words "vocabularies" of a long time series, we use a sliding window technique to convert a time series into the set of SAX words. By sliding a window across time series, extracting subsequences, converting them to SAX words, and placing these words into an unordered collection, we obtain the "Bag of Words" representation of the original time series (see Figure 3).

Each row of the constructed matrix (Bag of Words) represents a SAX word and corresponding frequency of that word generated by the sliding window procedure.

Following the common Information Retrieval workflow, we employ the TF*IDF weighting scheme for each element of this matrix in order to transform a frequency value into the weight coefficient.

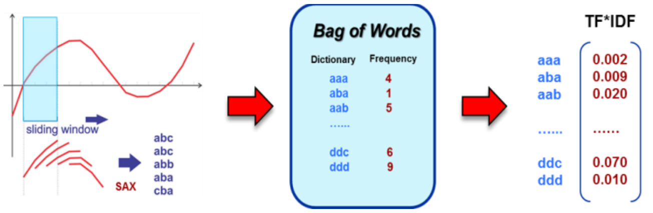


Figure 3. Sliding window allows to extract time subsequences and SAX converts them into words. By placing all words into an unordered collection, the original time series is represented by single bag of words. The bag of words can be replaced by a single weight vector representing TF*IDF statistics.

Similar to other classification techniques, SAX-VSM consists of two parts - the training phase and the classification procedure. An overview of the SAX-VSM algorithm (see [8] for details) is shown in Figure 4. In the training phase, all labeled time series from N training classes are transformed into symbolic representation, and the algorithm generates N TF*IDF weight vectors representing N training classes (see Figure 4).

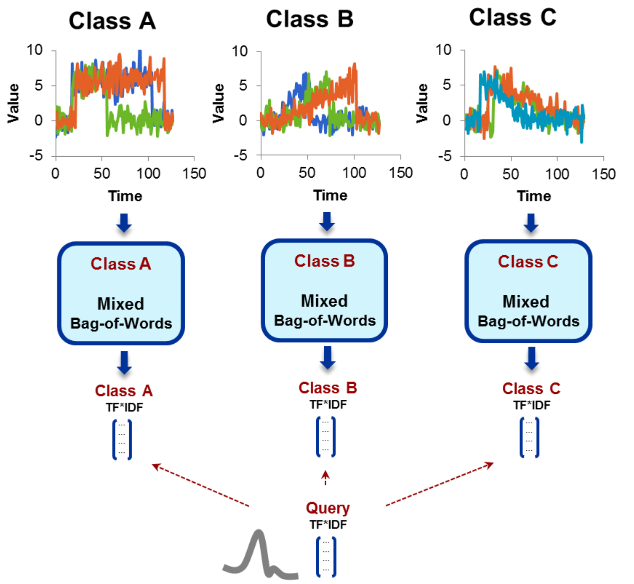


Figure 4. An overview of SAX-VSM algorithm: (i) all labeled time series from each class are converted first into a single bag of words using SAX and by TF*IDF statistics into a weight vector representing individual training class; (ii) for classification, an unlabeled time series is converted into a term frequency vector and assigned to the class whose TF*IDF weight vector yields a maximal cosine similarity value.

In the classification phase, an unlabeled time series is converted into a term frequency vector and assigned to the

ISBN: 978-1-61208-324-7

class whose TF*IDF weight vector has a maximal cosine similarity.

Detailed analysis of SAX-VSM performance and comparison with other temporal data classification techniques is described in detail in our original paper [8]. The unique characteristics of SAX-VSM, such as high classification accuracy, learning efficiency and a low computational complexity suggested using SAX-VSM for the goal of current research.

C. *Application of SAX-VSM for Multidimensional Time Series*

Our SAX-VSM algorithm [8] can be extended easily to the multi-dimensional case. Each dimension of multidimensional time series (trajectory) is processed independently in terms of calculating corresponding Bags-of-Words and TF*IDF weight vectors for each dimension. To compare two trajectories, *A* and *B*, cosine similarities along each dimension is calculated in the same way as it was done in one-dimensional case and then total similarity of the trajectories is estimated by combining similarities along all dimension :

$$sim(A,B) = \sqrt{\frac{\sum_{i=1}^{n} sim(A,B)_i^2}{n}} \qquad (1)$$

III. RESULTS

A. *Data Acquisition and Feature Extraction*

A Twitter™ data collection and feature extraction procedure was performed by an Indiana University team and described in detail somewhere [12]. The process can be summarized as follows. Two different classes of trending topics on Twitter™ were identified for study, promoted topics or advertisement campaigns and naturally trending topics (definitions of trending [13] and promoted [14] topics can be found on Twitter™ site). Advertising campaigns on Twitter™ were chosen because they represent good example of persuasion in social media, appear on Twitter™ systematically and represent an ideal testing scenario since it’s possible to collect and label data automatically. Twitter™ data were obtained thru the so-called gardenhose, getting approximately 10% randomly chosen subset from the total Twitter™ data stream. All trending hashtags appearing in the United States from January to April 2013 were recorded at regular 20 minutes interval and were automatically labeled by the system. The total number of promoted hashtags in the dataset collected by the system is 76 (with ~ 300 thousands tweets) while the number of naturally trending topics is 853 (~ 6 million tweets).

The time window of data collection was restricted from 7 days prior to the trending time and 1 day after. This configuration allows to generate a time-series consisting of up to 432 data points before the trending time point, and 72 points after that.

For each time point, three classes of different features were accumulated. They are network-based category of features, user-based features, and event-time-intervals features. The network-based category of features includes number of nodes/edges, density of network, in/out degree and etc., with statistical distributions of these features. Examples of user-based features are user followers, friends, and favorites. Examples of event-time-intervals features are time interval between two consecutive tweets, retweets, and mentions. Aggregating all features from all three categories produces an overall number of 224 features. Detailed description of all these features generated by the system of Indiana University can be found in [12].

B. *Classification Experiments*

In our classification tests, we used a well-known Leave-One-Out Cross-Validation (LOOCV) test in which the accuracy measures are obtained as follows. From the total set of samples (76 + 853 = 929), we take one for the test set, and use the remaining data for training. Applying multi-dimensional version of SAX-VSM classifier, we compute the accuracy for the test sample. We repeat the same procedure for all 929 samples and compute the mean accuracy.

There are three main challenges we have to address here: the first is the choice of data time window for analysis from available 8 days of data recording, the second is the choice of appropriate combination of retrieved features from total amount of 224, and the third is the choice of right parameters for SAX-VSM algorithm.

Our findings and conclusions described below are based on the empirical exploration of the problem and do not provide, at least for now, a comprehensive conclusion regarding the best strategy of parameter values choice. Below we describe the guidance and intuition we used in the parameter search.

The data time window can be described by two parameters, the offset relative to the starting point of topic trending point and the width of the time window. The initial choice was dictated by the need to get maximum signal level and is the following: the offset is equal to zero and the width of the window is equal to 70 data points that approximately covers one day starting from the begining of trending phase.

The SAX-VSM algorithm has three main parameters: data window width, PAA size and alphabet size. The later two parameters define approximation accuracy of SAX and their values are dictated by the specific profile shape of the time series (or its oscillation). The sliding window size defines the length of time series within the SAX compression procedure allowing to preserve the unique temporal sequence of oscillations of the time series. Our approach is based on many heuristic findings and guided by a trial-and-error strategy. As it was pointed out by authors of SAX [9], [10], sensitivity of SAX approximation to the choice of these parameters, both PAA and alphabet sizes, is not high and typical values of both PAA and alphabet sizes are within 4-8 range.

SAX-VSM parameter tuning was done manually by trial-and-error strategy. In the first step of our empirical strategy, we identified a few simple features demonstrating strong signal for most data samples, like frequency of tweets, density of retweet network, hashtag degree mean. Using LOOCV as an evaluation criteria, we started experiments varying randomly all these three parameters. It was not difficult to find out that reasonable values for those parameters are the following: W_{width}=70, N_{PPA}=4 and $N_{alphabet}$= 5.

The feature selection procedure was organized in the following way: we pipelined a Monte Carlo random search of feature combinations and LOOCV test. To reduce the search in potentially very large combinatorial space, we ranked individually all 224 features by their classification ability and then limited the search space by using only the 60 top features. We achieved good results in classification quality, keeping only 12 features and randomly testing possible combinations of 12 from the top 60 available features. The best features found this way are arranged according to their descending ranks and shown in Table 1. Together they produce classification accuracy of 97%. Leaving the first best six features for classification reduces the accuracy only by 3% (accuracy ~ 94%) while leaving only top three features, namely, hashtagN_degree_skiwness, hashtagN_CC_min and tweeting frequency, still gives reasonably good accuracy of ~ 92%.

It should be mentioned that the simple selection of the top 12 individually evaluated features does not produce the above quality level of accuracy. This is because many top features are significantly correlated and their combination does not improve their individual discrimination power but reduces accuracy by introducing additional noise.

TABLE I. SET OF MOST DESCRIMINATIVE TWITTER™ FEATURES*

Feature Name	Description
hashtagN_degree_skewness	Skewness of degree distribution (hashtag network)
hashtagN_CC_min	Min. clustering coeff. (hashtag network)
Frequency	Volume of tweets
mentionN_LCC_mean_shortest_path	Mean shortest-path (LCC) of the mention network
retweetN_density	Density of the retweet network
event_interval_mean	Mean of distribution of tweets time intervals
hashtagN_degree_entropy	Entropy of degree distribution (hashtag network)
event_retweet_interval_kurtosis	Kurtosis of distribution of retweets time intervals
user_favourites_count_min	Min. of distribution of favorite tweets
event_mention_interval_entropy	Entropy of distribution of mentions time intervals
event_mention_interval_std	Std. dev. of distribution of mentions time intervals
event_interval_skewness	Skewness of distribution of tweets time intervals

*The features are arranged according to their descending ranks.

To evaluate the performance of binary classifying systems like our SAX-VSM procedure, it is a common practice to calculate a Receiver Operating Characteristic (ROC), or ROC curve. By plotting the true positive rate vs. the false positive rate at various threshold settings and measuring the area under the ROC curve (AUC), we get another evaluation of classifier accuracy. In Figure 5, the plot of the ROC is shown for the case of 12 features included in Table 1.

The encouraging results presented above indicate that the classification task of promoted and non-promoted topics can be done with a high accuracy at trending phase on Twitter™. But it would be more challenging to be able to predict a situation by labeling the topic as abnormal before it becomes trending and attracts a large audience.

We performed a few experiments with the goal to achieve a reasonably good classification using the data from a time window located before trending point. To explore the possibility of early detection of promoted topics, we shifted the time window systematically forward as far as possible from the trend starting point while trying to reduce the width of the window. The limited number of experiments was done by varying these two parameters: location of time window and its width. It was not surprising that classification accuracy dropped due to diminishing the signal quality. Nevertheless, after multiple tests we found that the best results can be achieved with a time window of 35 points wide, located 35 points (~ half day) before trending begins

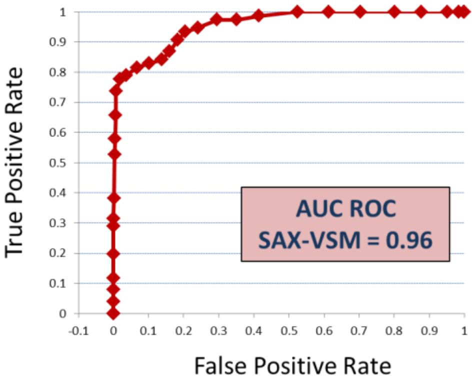


Figure 5. The ROC curve for Twitter™ topic classification by SAX-VSM and using combination of 12 most descriminative features included in the Table 1. The area under the ROC curve (AUC ROC) is indicated in the inset.

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-324-7

(W_{width}=35, W_{offset}=35). The classification accuracy with this setting is approximately 82%.

At this stage, it is beyond of the scope of our studies to perform exhaustive analysis of optimal SAX-VSM configuration, as well as to consider alternative classification approaches. A comparison of SAX-VSM with a few different classifiers can be found in our expanded report [12]). For now, the obtained results at least indicate that early detection can be done with a reasonable level of accuracy.

IV. RELATED WORK

To the best of our knowledge, the work is the first successful attempt at using temporal characteristics of user networks to detect orchestrated influence in online social networks.

Several research studies were focused on the dynamics of information flow through online social networks [15], [16], [17], [18]. In social networks, the relationships and interactions within a group of individuals plays a fundamental role as a medium for the spread of ideas and influence among its members. The close relation between structure of social networks and spread of information has been observed in various studies, including modeling approaches [2], [19], [20], [21].

Temporal dynamics of information diffusion was reliably predicted by simple Linear Influence Model [20]. A model of epidemics spread on networks [21] was applied to characterize the spread of topics through the blogosphere [18]. Building systems that use models of the Blogosphere allow to recognize spam blogs, find opinions on topics, identify communities of interest, and detect influential bloggers [2].

Temporal behavior of trending topics [22], [23] was explored in extensive studies where the entire Twitter™ site with 41.7 million user profiles, 4,262 trending topics, and 106 million tweets, was crawled [1]. The trending topics by definition are the topics that are immediately popular, rather than topics that have been popular for a while. Analysis of retweets in trending topics reveals that any retweeted tweet is to reach an average of 1000 users no matter what the number of followers is of the original tweet. The chain of retweets grows almost instantly after the first retweet, which explains the fast diffusion of information.

Prediction of trending topics on Twitter™ was done recently by a simple data-driven model [24], [25]. The algorithm analyzes the temporal trace of tweeting frequency for each topic and compares that trace to the one for every sample in the training set. Statistical resemblance of a test topic is calculated for all training examples and the combined weighting function suggests the likelihood that a new topic would trend. The algorithm predicts trending topics with the accuracy ~ 79% and about ~ 1.5 hour before they appear on Twitter™.

A few studies explored the relationship of temporal dynamics of meme propagation and statistics of time intervals between social media events. A novel technique for detecting spam blogs or splogs, based on the observation that a blog is a dynamic and growing sequence of posts rather than a collection of individual pages, was developed in [26]. The detection of splog is performed by using temporal and structural regularity of content, posting time and links.

Ghosh et al. [27] showed that the analysis of retweeting activity only (distribution of event time intervals), without any knowledge of tweet content, allows for the identification of several different types of activity, including marketing campaigns, information dissemination, auto-tweeting, and spam. Lerman and Ghosh [15] showed that the patterns of information propagation strongly depend on the type of topic.

Related to our work is also the study made on detection of astroturfing in social media [4], [5]. Astroturfing (false grassroots) campaigns are examples of deceptive orchestrated campaigns with a goal to promote some ideas by creating fake accounts, hiding identities and locations of users to give the impression of widespread support for their agenda. It was shown that certain network features and topological patterns are highly predictive of astroturfing [5].

V. CONCLUSIONS AND FEATURE WORKS

In this paper, we presented a novel approach for detection of persuasion campaigns in online social networks. We demonstrated that without any content analysis of topics on Twitter™, by monitoring only temporal traces of topological characteristics of users' networks with twitting temporal activity, it is possible to distinguish two types of topics on Twitter™, promoted or advertisement campaigns and non-promoted or naturally trending topics. We presented experimental results of applying our SAX-VSM classification technique of multidimensional time series to achieve high detection accuracy on Twitter™ data. Our results suggest that social streams can be monitored effectively almost in a real time and some abnormal activity can be detected by analyzing temporal evolution of social networks.

For our future work, we consider undertaking a detailed analysis of factors affecting the accuracy of detection and time-prediction of influencing in social media and understand details of underlying processes.

ACKNOWLEDGMENT

The author would like to thank Indiana University team who provided us with Twitter™ data and collaborated closely in the course of the project. Specifically, we are thankful to Onur Varol who worked on data acquisition and feature retrieval; and to Filippo Menczer, Alessandro Flammini and Emilio Ferrara for helpful discussions. Also we are thankful to Pavel Senin, PhD student of University of Hawaii, for very productive joint work on SAX-VSM technology and to Paul Biancaniello for discussion of the concept at early stage. This work is supported by DARPA grant W911NF-12-1-0037 / PO#1099798.

REFERENCES

[1] H. Kwak, C. Lee, H. Park, and S. Moon, “What is Twitter, a social network or a news media?,” Proc. 19th international conference on World Wide Web, ACM, 2010, pp. 591-600.

[2] T. Finin et al., “The Information Ecology of Social Media and Online Communities,” AI Magazine, 2008, vol. 29, no 3, pp. 77-92.

[3] E. Bakshy, J. M. Hofman, W. A. Mason, and D. J. Watts, “Everyone's an in influencer: quantifying influence on Twitter,” Proc. fourth ACM international conference on Web search and data mining, ACM, 2011, pp. 65-74.

[4] J. Ratkiewicz et al., “Detecting and tracking political abuse in social media,” Proc. 5th International AAAI Conference on Weblogs and Social Media, 2011.

[5] J. Ratkiewicz et al., “Truthy: mapping the spread of astroturf in microblog streams,” Proc. 20th International Conference Companion on World Wide Web, ACM, 2011, pp. 249-252.

[6] V. Qazvinian, E. Rosengren, D. R. Radev, and Q. Mei, “Rumor has it: Identifying misinformation in microblogs,” Proc. Conference on Empirical Methods in Natural Language Processing, ACL, 2011, pp. 1589-1599.

[7] C. Wagner, S. Mitter, C. Korner, and M. Strohmaier, “When social bots attack: Modeling susceptibility of users in online social networks,” Proc. 21th International Conference Companion on World Wide Web, 2012.

[8] P. Senin and S. Malinchik, “SAX-VSM: Interpretable Time Series Classification Using SAX and Vector Space Model“, Proc. ICDM 2013, Dallas, Texas / December 7-10, 2013.

[9] J. Lin, E. Keogh, S. Lonardi, and B. Chiu, “A symbolic representation of time series, with implications for streaming algorithms,” Proc. 8th ACM workshop on Research Issues in Data Mining and Knowledge Discovery, 2013, pp. 2-11.

[10] J. Lin, E. Keogh, L. Wei, and S. Lonardi, “Experiencing SAX: a novel symbolic representation of time series,” Proc. Data Mining and Knowledge Discovery, 15(2), 2007, pp. 107-144.

[11] G. Salton, A. Wong, and C. S. Yang, “A vector space model for automatic indexing,” Communications of the ACM, 18(11), 1975, pp. 613-620.

[12] E. Ferrara, O. Varol, S. Malinchik, F. Menczer, and A. Flammini, “Toward detecting persuasion campaigns in social media,” Proc. 8th International AAAI Conference on Weblogs and Social Media, ICWSM’14, 2014 (under review).

[13] https://support.twitter.com/articles/101125-faqs-about-twitter-s-trends

[14] https://support.twitter.com/articles/282142-what-are-promoted-trends

[15] K. Lerman and R. Ghosh, “Information contagion: An empirical study of the spread of news on Digg and Twitter social networks,” Proc. ICWSM, 2010, pp. 90-97.

[16] D. M. Romero, C. Tan, and J. Kleinberg, “On the interplay between social and topical structure,” Proc. 7th International AAAI Conference on Weblogs and Social Media, 2013.

[17] D. M. Romero, B. Meeder, and J. Kleinberg, “Differences in the mechanics of information diffusion across topics: idioms, political hashtags, and complex contagion on twitter,” Proc. 20th International Conference on World Wide Web (WWW'11), 2011, pp. 695-704.

[18] D. Gruhl and D. Liben-Nowell, “Information diffusion through blogspace,” Proc. Int. World Wide Web Conference (WWW) , 2004, pp. 491– 501.

[19] D. Kempe, J. Kleinberg, and É. Tardos, “Maximizing the spread of influence through a social network,” Proc. 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '03), 2003, pp. 137-146.

[20] J. Yang and J. Leskovec, “Modeling Information Diffusion in Implicit Networks,” Proc. 2010 IEEE 10th International Conference on Data Mining (ICDM), 13-17 Dec., 2010, pp. 599-608.

[21] M. E. J. Newman, “Spread of epidemic disease on networks,” Physical Review E, 66(1), 2002, 016128.

[22] C. Budak, D. Agrawal, and A. El Abbadi, “Structural trend analysis for online social networks,” Proc. VLDB Endowment, 4(10), 2011, pp. 646- 656.

[23] J. Leskovec, L. Backstrom, and J. Kleinberg, “Meme-tracking and the dynamics of the news cycle,” Proc. 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM, 2009, pp. 497-506.

[24] S. Nikolov, “Trend or no trend: A novel nonparametric method for classifying time series,” PhD Thesis, MIT, 2012.

[25] S. Nikolov and D. Shah, “A Nonparametric Method for Early Detection of Trending Topics,” MIT, 2012, http://web.mit.edu/snikolov/Public/NikolovShahWIDS2012.pdf

[26] Y. Lin, H. Sundaram, Y. Chi, J. Tatemura, and B. Tseng, “Detecting splogs via temporal dynamics using self-similarity analysis,” Proc. ACM Transactions on the Web (TWEB), 2(1), 2008, pp. 1–35.

[27] R. Ghosh, T. Surachawala, and K. Lerman, “Entropy-based classification of ’retweeting’ activity on twitter,” Proc. KDD workshop on Social Network Analysis (SNA-KDD), 2011, pp.17-23.

Estimating the Representativeness of German Parties in the 2013 Bundestag Election

Andranik Tangian
WSI (Institute for Social and Economic Research) in the Hans-Böckler-Foundation
Düsseldorf, Germany
and Karlsruhe Institute of Technology
andranik-tangian@boeckler.de

***Abstract*—The positions of German parties on 36 policy issues are compared with the results of public opinion polls, and the parties' indices of popularity (the average percentage of the population represented) and universality (frequency in representing a majority) are constructed. The 2013 federal election winner, the CDU/CSU, is shown to be the least representative among the 28 paries considered. The most representative among the four parties in the Bundestag (with >5% of the votes) is DIE LINKE, which received only 8.6% of the votes. It is concluded that voters are inconsistent with their own political profiles, disregard party manifestos, and are likely driven by political traditions, even if outdated, or by personal images of politicians.**

***Keywords*-Mathematical theory of democracy; German parties; Bundestag election 2013; indices of representativeness.**

I. Introduction

Table I shows the four German paries which, having received $> 5\%$ of the votes in the 2013 federal election, are eligible for the Bundestag seats. The goal of the paper is estimating the representativeness of these and other German parties participating in the 2013 Bundestag election from the viewpoint of direct democracy. For this purpose, we compare the parties' positions on topical policy issues with the outcomes of public opinion polls and construct the parties' indices of popularity (the average percentage of the population represented) and universality (frequency in representing a majority), according the methodology described in [5].

The party positions are taken from the Wahl-O-Mat — an internet site of the Bundeszentrale für politische Bildung (German Federal Agency for Civic Education) [2]. Recall that the Wahl-O-Mat (an invented word composed from the German *Wahl* = election and *Automat*) is the German version of the Dutch Internet site *StemWijzer* ('VoteMatch') [3], which was originally developed in the 1990s to involve young people in political participation. Both websites help the users locate themselves on the political landscape by testing how well their opinions fit with party positions. Before an election (local, regional, federal, and even European), a special governmental supervising committee compiles a list of questions on topical policy issues ('Introduce minimum wage?'—Yes/No, 'Introduce a general speed limit on motorways?'—Yes/No, etc.) and asks the parties participating in the election for their answers. A user of the site answers the same questions, eventually attributing weights to reflect their importance, and then the program compares his or her political profile with that of the parties and finds the best-fitting party, the next best-fitting party, etc. No statistical data are available form the Wahl-O-Mat, and if any were available, they would be biased toward internet users. Therefore, by any reason, the balance of public opinion is better reflected by relevant public opinion polls.

Table I
RESULTS OF 2013 GERMAN BUNDESTAG ELECTION

	CDU/CSU	SPD	DIE LINKE	GRÜNE	25 parties ineligible for Bundestag seats ($< 5\%$ of the votes)
Votes (%)	41.6	25.8	8.6	8.4	15.7
Bundestag seats (%)	49.3	30.6	10.1	10.0	

CDU/CSU	Union of Germany's two main conservative parties, Christlich Demokratische Union Deutschlands (Christian Democratic Union of Germany) and Christlich-Soziale Union in Bayern (Christian Social Union of Bavaria)
SPD	Sozialdemokratische Partei Deutschlands (Social Democratic Party of Germany)
DIE LINKE (The Left)	the 1997 merger of East German communists and the Electoral Alternative for Labour and Social Justice (WASG), a left-wing breakaway from the SPD
GRÜNE (The Green)	BÜNDNIS 90/DIE GRÜNEN (Alliance 90/The Greens) the merger of two ecologically-focused parties, DIE GRÜNEN (West Germany) and BÜNDNIS 90 (East Germany), both with a social-democratic background

Source: [1], [2]

For the given model, we consider the Wahl-O-Mat answers of 28 German parties participating in the 2013 Bundestag election and the results of 36 public opinion polls relevant to 36 out of 38 Wahl-O-Mat questions. The full information on the party answers with their comments on them as well as on the public opinion polls with all the references is given in the report [4].

II. Construction of indices

Figure 1 shows the balance of public and Bundestag opinions on 38 topical policy issues, as well as the position of the DGB (Confederation of German trade unions).

To explain the figure, consider the top question: '1. Introduce a nationwide minimum wage'. The question number

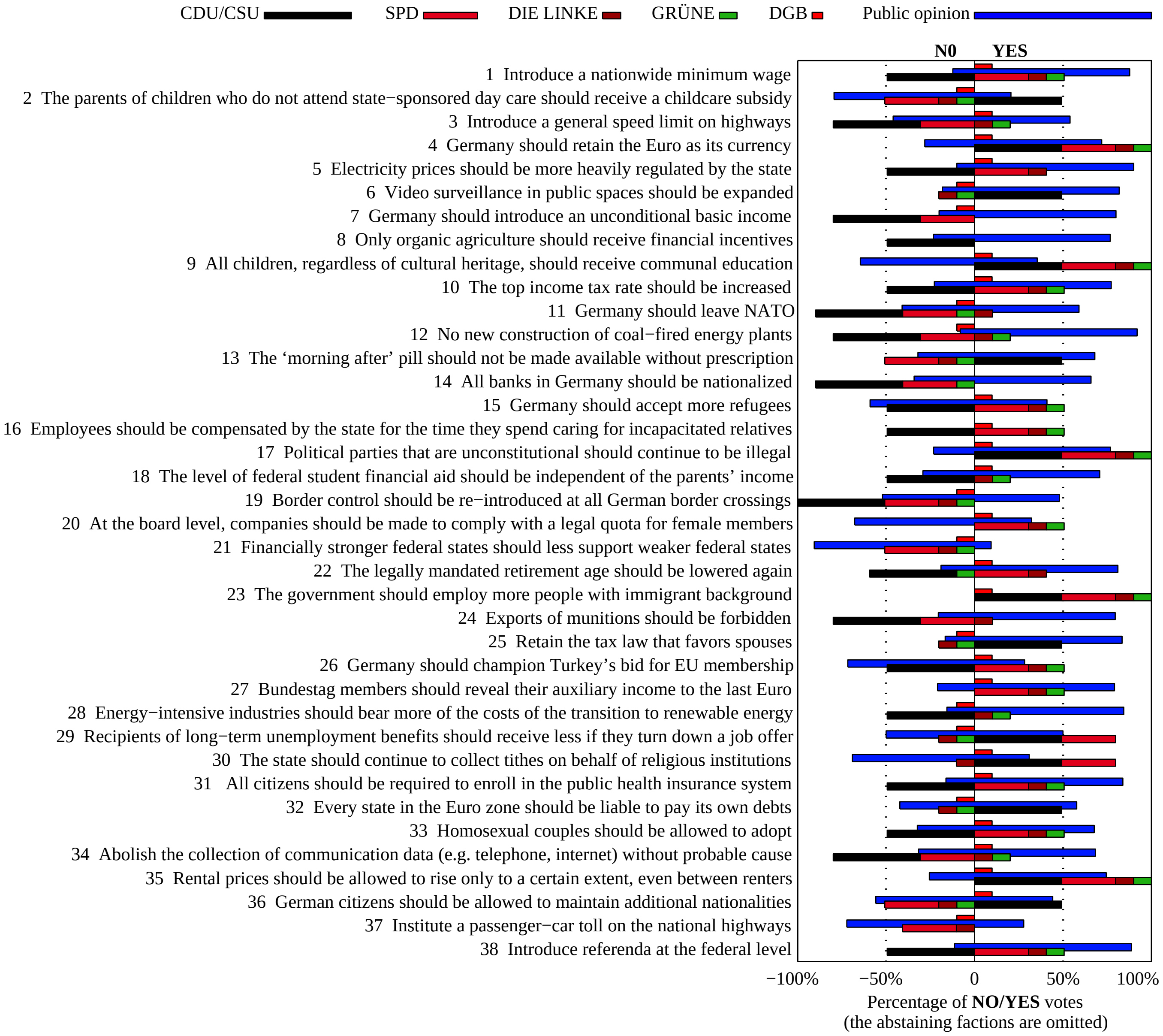


Figure 1. Public opinion and representation thereof by the 2013 Bundestag and the DGB

'1' is as in the 'official' *Wahl-O-Mat* questionnaire filled by the parties shortly before the Bundestag elections 2013.

The small red rectangle above the blue bar shows the Yes/No position of the DGB, which does not participate in the election but nevertheless has a position on the issue.

The balance of public opinion 86% : 12% on the issue is shown by the blue bar whose length is normalized to 100% (abstaining respondents are ignored). The size of the bar to the left side and to the right side of the central axis correspond to the percentage of antagonists and protagonists in the society, respectively. The blue bar's bias from the center indicates at the prevailing public opinion.

A Bundestag faction is depicted by a rectangle with the 'official' party color. Its length is proportional to the number of the party seats in the Bundestag. The 'No/Yes' party opinion on the question is reflected by the location of the rectangle to the left side or to the right side from the central vertical axis, respectively. A Bundestag majority is attained if the cumulative length of party rectangles surpasses the 50%-threshold (marked with dotted lines).

If the position of DGB, public, or party is unknown, the corresponding rectangle is missing.

Table II
CORRELATION BETWEEN THE PARTY RANKS WITH RESPECT TO THE INDICES (RANK CORRELATIONS)

		Votes	Popularity				Universality			
			unweighted	Google	Brigitte Unger	Anne Graef	unweighted	Google	Brigitte Unger	Anne Graef
Votes		1.00	−0.29	−0.27	−0.30	−0.26	−0.34	−0.33	−0.31	−0.29
Popularity	unweighted	−0.29	1.00	0.99	0.98	0.94	0.98	0.98	0.98	0.94
	Google	−0.27	0.99	1.00	0.98	0.95	0.96	0.98	0.98	0.95
	Brigitte Unger	−0.30	0.98	0.98	1.00	0.96	0.95	0.96	0.99	0.95
	Anne Graef	−0.26	0.94	0.95	0.96	1.00	0.92	0.94	0.95	0.97
Universality	unweighted	−0.34	0.98	0.96	0.95	0.92	1.00	0.99	0.98	0.96
	Google	−0.33	0.98	0.98	0.96	0.94	0.99	1.00	0.98	0.96
	Brigitte Unger	−0.31	0.98	0.98	0.99	0.95	0.98	0.98	1.00	0.96
	Anne Graef	−0.29	0.94	0.95	0.95	0.97	0.96	0.96	0.96	1.00

Let us show how these data are used to construct the party indices of representativeness. For every question, a given party represents a certain fraction of the population (identified with the fraction in the opinion polls). For instance, the CDU/CSU with their ‘No’ answer to the first question ‘1 Introduce nation wide minimum wage’ represents the opinion of 12% of the population versus 86%. After removal of abstaining respondents and normalization, we obtain the CDU/CSU *representativeness* for Question 1:

$$r_{\text{CDU/CSU,1}} = \frac{12}{12+86} \times 100\% \approx 12.2\% \ .$$

Similarly, with the ‘Yes’ answer to the next question ‘2 The parents of children who do not attend day care should receive a childcare subsidy’, the CDU/CSU expresses the opinion of 20% of the population versus 77%. After removal of abstaining respondents and normalization we obtain the CDU/CSU representativeness for Question 2:

$$r_{\text{CDU/CSU,2}} = \frac{20}{20+77} \times 100\% \approx 20.6\% \ ,$$

and so on. Taking the average representativeness of the CDU/CSU over the questions with known results of public opinion polls and definitive party responses (there are 36 such questions), we obtain the party’s unweighted *popularity* index

$$\mathsf{P}_{\text{CDU/CSU}} = \frac{12.2+20.6+\cdots}{32} \times 100\% \approx 40\% \ .$$

A higher popularity means that, on average, a larger fraction of the electorate is represented. Taking the average with the weights, we obtain weighted versions of popularity. (For every party, the questions with missing opinion polls or party positions are removed from consideration, and the question weights are proportionally adjusted to the total of 100%.)

The frequency in representing a majority ($\geq 50\%$) is defined to be the unweighted *universality* of the party. The CDU/CSU represents a (non-strict) majority on 11 out of 32 questions that are backed up by public opinion polls and the CDU/CSU positions. Hence, the frequency in representing a majority is

$$\mathsf{U}_{\text{CDU/CSU}} = \frac{11}{32} \times 100\% \approx 34\% \ .$$

A higher universality means that a majority is represented more frequently. If the questions are counted with weights, we obtain the weighted versions of the universality index.

Figure 2 displays the indices of popularity P and universality U for 28 German parties parties, DGB and Bundestag in four versions each: unweighted questions (marked in the subsequent charts by ‘u’), weighted by the logarithm with base 2 of the number of Google hits for the questions’ keywords (marked by ‘g’), assuming that the number of relevant documents in the Internet reflects the importance of the question, and weighted by two experts — the director of the Institute for Economic and Social Research in the Hans-Böckler-Foundation, Professor Brigitte Unger, and the editor-in-chef of the DGB info-service *Einblick*, Anne Graef (marked by ‘b’ and ‘a’, respectively). The parties are sorted in the decreasing order of the mean of all the eight indices. The correlations between the party ranks with respect to the indices (rank correlations) are shown in Table II.

III. CONCLUSIONS

Inconsistency of election results with public opinion: As one can see, the winner of the 2013 Bundestag election, the conservative party CDU/CSU with 41.6% of the votes, has the lowest ranking among all the 28 parties considered. Correspondingly, it also ranks lowest among the four eligible parties. The most representative among the eligible parties is DIE LINKE, which received only 8.6% of the votes. The negative correlations between the party ranks with respect to the votes received and the indices of representativeness show that most electors vote inconsistently with their own political profiles. A possible explanation of this inconsistency is the significant shift of the German (and world) political spectrum to the right after the 1990 German reunification and collapse of communism, although voters still believe that the parties represent the same values as a few decades ago.

Weak dependence between public opinion and the Bundestag position: Note that the Bundestag’s representative capacity is estimated at about 50%. It should be realized that 50% of representativeness is expected when, for every issue, a coin is tossed whose sides indicate the decisions in

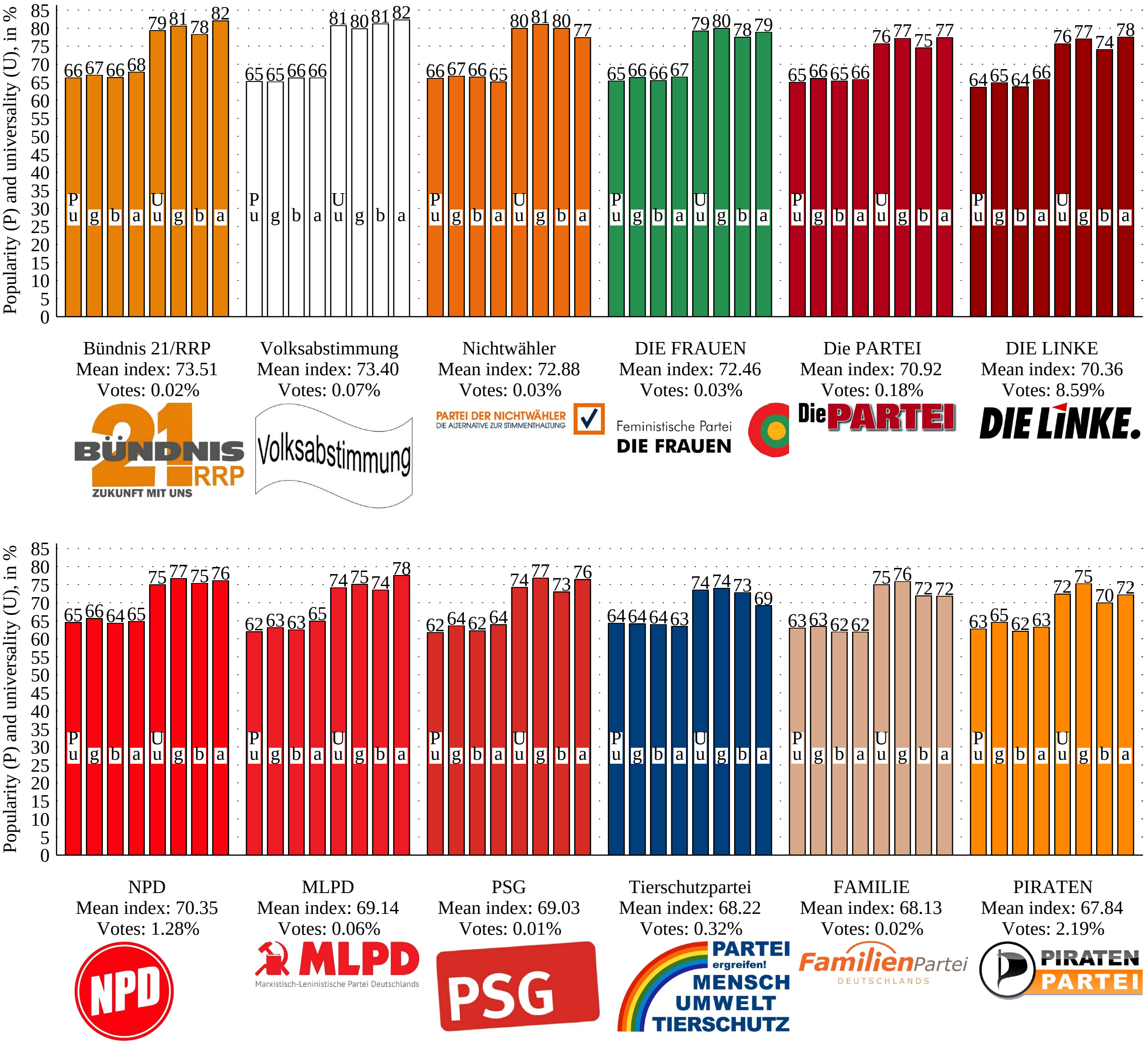


Figure 2. Indices of German parties and the DGB: P—popularity, U—universality, u—for unweighted questions, g—for questions weighted by the number of Google hits, b—for questions weighted by Brigitte Unger as the first expert, and a—for questions weighted by Anne Graef as the second expert

favor of either the majority or the minority in the society. Therefore, the index values of about 50% can be interpreted as the lack of dependence between public opinion and the Bundestag position.

Warning for policymakers: All of these constitute a serious warning against the use of traditional voting methods for selecting representatives of public opinion. Among other things, 'wrong voting' gives faulty feedback to policymakers about the policies they pursue. Already now, both extreme right and extreme left parties rank much higher than the moderate parties currently elected to the Bundestag. However, this cannot last forever, and if the discrepancy between the population and the government becomes critical, an extremist government can be elected.

Secondary role of weighting: In Table II, all the rank correlations between the indices of representativeness are very close to one. Even the correlation between the unweighted and the Google-weighted indices — with the extremes in weight ranging from 42,900 (for Question 9 about separate school lessons for children with different cultural background) to 31,600,000 (for Question 31 about merging statutory and private health insurances) — is 0.99 or 0.98. This means that the party ranks are not very sensitive to the question weighting.

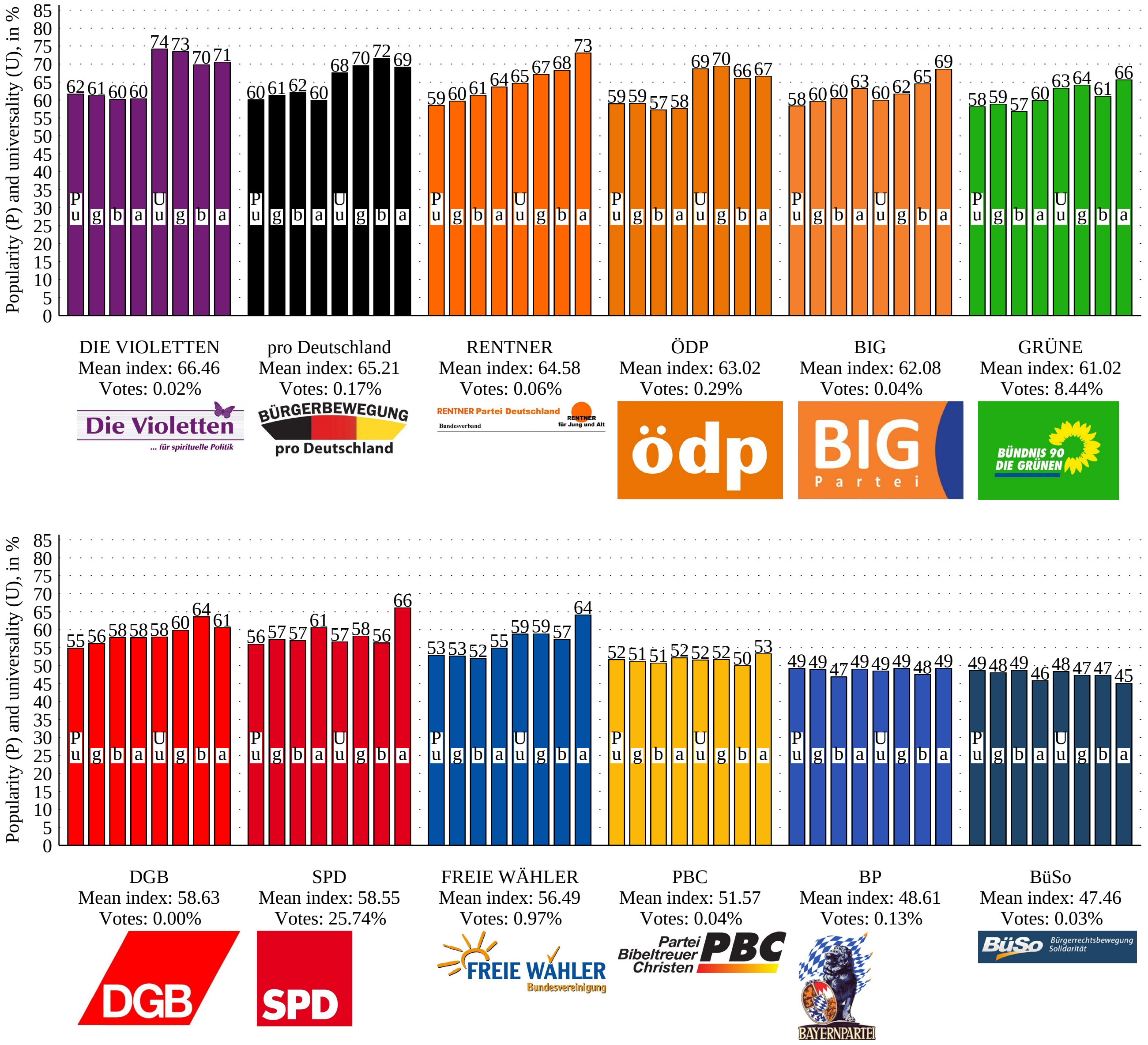


Figure 2. (continued) Indices of German parties and the DGB: P—popularity, U—universality, u—for unweighted questions, g—for questions weighted by the number of Google hits, b—for questions weighted by Brigitte Unger as the first expert, and a—for questions weighted by Anne Graef as the second expert

The similarity in index orders can be explained as follows. The responses of a given party are backed up by the party ‘ideology’, which determines the high intra-question correlations of party answers. Therefore, ‘erroneous’ weighting and even omission of some questions play a rather negligible role, because other questions carry superfluous information on the party political profile. Hence, we can evaluate the parties by the mean of its eight indices as done in Figure 2, or by the most ‘impartial’ unweighted indices.

Evaluation of representatives without election: The known DGB position on the given policy issues allows us to evaluate its popularity and universality, although the DGB does not participate in elections. In the same way, the representativeness of any political body can be evaluated without elections, just by comparing its position with the results of public opinion polls.

IV. Discussion: How to improve election

The approach developed in this paper prompts a way to improve the election procedure. The aim is (a) to redirect the voters’ attention from candidate (party) images to their manifestos as political profiles, and (b) to base the election

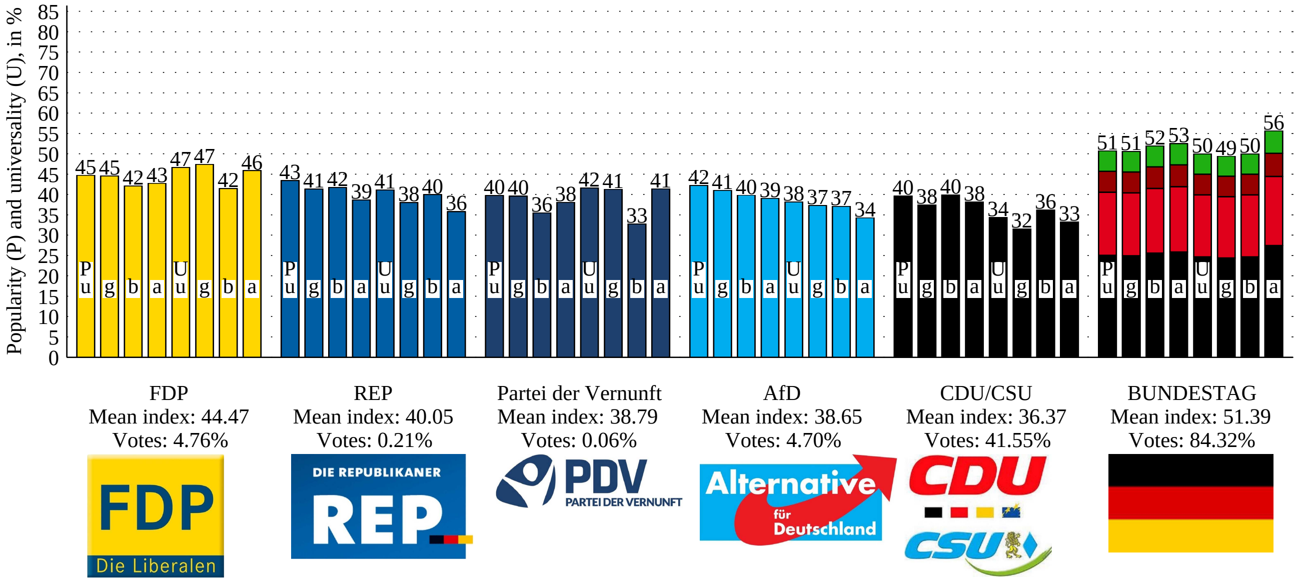


Figure 2. (continued) Indices of German parties and the DGB: P—popularity, U—universality, u—for unweighted questions, g—for questions weighted by the number of Google hits, b—for questions weighted by Brigitte Unger as the first expert, and a—for questions weighted by Anne Graef as the second expert

of candidates on matching their profiles to the majority will.

Currently the Bundestag is elected with two votes, the first *(Erststimme)* for a person and the second *(Zweitstimme)* for a party. The first 299 Bundestag members are representatives of local constituencies elected through the first vote. The next 299 Bundestag seats are distributed among the eligible parties (who have at least 5% of the second votes) to form their factions, including the party members. Thus, the second vote is decisive because it determines the size of Bundestag factions already elected by the first vote, in proportion to the second votes. Thereby, the partiality of the vote for a person is reduced by rearranging the Bundestag factions according to the more impersonal second vote for a party.

This logic of increasing impartiality of votes can be continued by introducing the absolutely impartial third vote *(Drittstimme)* asking for the elector's political profile. It is imagined in the form of a survey on selected points of the party manifestos (Introduce nationwide minimum wage? Yes/No; etc.). As explained previously, the political profiles of the candidates (parties) are backed up by certain ideologies, making the answers to different questions strongly interdependent. Therefore, a few questions suffice to specify the political profiles of both candidates and voters.

In other words, we propose to combine elections with referenda revealing the public opinion on a sample of issues. The suggested approach envisages processing the totality of the ballots and evaluating candidates with respect to the fit of their manifestos to the public profile. It should be noted that in Switzerland, Canada and United States, referenda are often coupled with elections, however, not as criteria to distribute parliament seats or public offices but rather for the convenience of the population.

Of course, a practical implementation should not exclude traditional ways of expressing opinions. In addition to questionnaires in the ballots, direct votes for a candidate and for a party should remain an option. Note that such a voting duality is already inherent in the German parliamentary election system with the first vote for a specific person, and the second vote for a party. In our consideration, the vote for a party is complemented with a vote for an even more impersonal party manifesto. Of course, one can also imagine a mixed procedure where the allocation of the Bundestag seats is derived from both the second votes and the party indices obtained through the third votes.

References

[1] Bundeswahlleiter (2013) Ergebnisse der Wahl zum 18. Deutschen Bundestag. http://www.bundeswahlleiter.de/de/bundestagswahlen/. Cited 23 October 2013

[2] Bundeszentrale für politische Bildung (2013). Wahl-O-Mat. http://www.bpb.de/methodik/XQJYR3. Cited 23 October 2013

[3] Institute for Public and Politics (2010) StemWijzer. http://www.stemwijzer.nl/. Cited 3 May 2013.

[4] A. Tangian, Decision making in politics and economics: 5. 2013 Election to German Bundestag and direct democracy. Karlsruhe Institute of Technology, Working Paper 49, 2013.

[5] A. Tangian, Mathematical Theory of Democracy. Berlin–Heidelberg: Springer, 2014.

Semantic Integration of Sensor Measurements and Human Self-observations for Physical-Cyber-Social Computing

Artem Katasonov, Jarkko Leino and Timo Tuomisto

VTT Technical Research Centre of Finland
Tampere, Finland
e-mail: artem.katasonov@vtt.fi, jarkko.leino@vtt.fi, timo.tuomisto@vtt.fi

***Abstract*—To deliver on their promises, Physical-Cyber-Social systems must semantically integrate a wide range of heterogeneous multimodal observations, including physical sensor measurements, human self-observations, social observations, and demographic observations. In this paper, we address the problem of collecting and combining sensor measurements and self-observations. We describe an architecture, main features of which are a triple-space-based approach to data integration and a novel approach utilizing instant messaging for eliciting self-observations. A specific application domain considered is health-related monitoring of elderly persons at their homes.**

Keywords – physical-cyber-social; smart home; data integration; assisted living

I. Introduction

Amit Sheth has recently popularized the concept of *Physical-Cyber-Social (PCS) computing* [1] as an emerging paradigm supported by the expanding Internet of Things (an improved ability to observe the physical world), cyberspace (an improved ability to access a massive repository of background knowledge on the Web), and social media (improved access to social knowledge). [1] claimed that PCS will be able to address in a holistic manner questions that neither human intelligence nor present computing systems can answer. In healthcare, for example, this could mean a highly personalised interpretation of a blood pressure reading and personalised suggestions of corrective actions. More generally, the combination of cyber-physical and social data can help us to understand events and changes in our surrounding environments better, monitor and control buildings, homes and city infrastructures, provide better healthcare and elderly care services among many other applications [2].

[1] states that in order to achieve its goals, PCS must access and semantically integrate a wide range of heterogeneous multimodal observations, including physical sensor measurements (such as blood pressure or heart rate), self-observations (subjective states and sensations), social observations (from a network including family, friends, and colleagues), and demographic observations (aggregated characteristics of the population with similar attributes or lineage). In addition to such integration of observations performed by PCS horizontal operators [1], there is a need for PCS vertical operators to progressively lift the integrated observations along the Data-Information-Knowledge-Wisdom dimension. Horizontal operators deal with variety and veracity of data, while vertical operators deal with its volume and velocity.

In this paper, we introduce a software architecture aiming to provide one required horizontal operator for PCS systems that is the collection and semantic integration of physical sensor measurements and human-produced observations, in particular, self-observations. The main features of this architecture include a triple-space-based approach to open interconnected systems [3], use of W3C's Semantic Sensor Network (SSN) ontology [4], an automation framework for triple-space management, a novel approach utilizing instant messaging for eliciting human-produced observations and integrating them with the rest of data, and optional integration of the speech interface within the latter. Collection and processing of human observations has been a rapidly growing research area [5] but focused on the analysis of unsolicited observation streams, e.g., from Twitter. To the best of our knowledge, there exists no streamlined approach to collecting solicited human observations and integrating them with physical sensor measurements.

The rest of the paper is structured as follows. Section II describes one motivating scenario for this work, namely health-related monitoring of an elderly person at home. Section III specifies the main components of our data integration architecture, with a brief discussion of related security aspects. Section IV follows with a description of our approach to collecting self-observations, including how we integrate a speech-based interface as a part of it. Finally, Section V concludes the paper.

II. Motivating Case: USEFIL

This work is performed in and motivated by the application domain of the EU FP7 project *Unobtrusive Smart Environments for Independent Living (USEFIL)* [6], [7].

The life expectancy in the EU and in other developed countries is continuously increasing and the proportion of elderly citizens in the population is growing. The elderly are often living alone, approximately one of every three non-institutionalized older adults [8], and often cannot afford private carers. Prolonging their ability to remain independently in their homes may yield economic and emotional benefits at the societal and personal levels. On the other hand, elderly are prone to decline in physical abilities, chronic illnesses, cognitive decline, and depression. Therefore, responsibly postponing their move into a nursing home requires maintaining a continuous confidence in their ability of independent and safe living.

The most common reasons elderly are admitted into nursing homes are caregiver burden and the elderly person's inability to perform Activities of Daily Living (ADLs) such as moving around, dressing, or bathing [9]. The elderly are also especially affected by loneliness and depression brought on by the Empty Nest Syndrome or neglect, either intentional or not [9]. In line with this, the main objective of the USEFIL project is to provide low-cost ICT solutions for monitoring physical health, cognitive health and emotional status of elderly (65+ years old) with age related disabilities at their homes – to assess their ability of independent living and to detect deteriorations when they occur. In addition, USEFIL aims at facilitating elderly access to telecare, as well as supporting their social interactions to fight loneliness.

The setup of the USEFIL system allows for various physical sensors. A central role is played by imaging devices: a video camera placed behind a mirror and a depth sensor such as Microsoft Kinect. The project develops algorithms to extract from those data various ADL parameters, such as walking balance and ability of transfer (e.g., raising from a chair), health signs, such as heart rate and pupils equality (relevant to stroke patients), as well as emotional states. In addition, USEFIL features a wrist wearable unit (Android watch-phone) with custom algorithms for processing accelerometer data to recognize and monitor daily activities.

As end-user interfaces, USEFIL employs a Smart TV and a tablet computer. Both provide a user interface for data access (health trends, medication schedule and reminders, etc.) as well as communication channels, both to healthcare and to family/friends. The wrist unit also provides a limited user interface allowing receiving messages as well as including a software ”panic” button.

In addition to physical sensors for unobtrusive monitoring, USEFIL realized a need for collecting self-observations, where the monitored elderly person is posed one or more questions to answer using either TV or tablet interface. Self-observations complement the physical sensor observations and are needed, in particular, for accessing the emotional status of an elderly person and detecting depression.

The USEFIL system includes data fusion and Decision Support System components which are responsible for abstracting the data, thus can be seen as PCS vertical operators (see Section I). In the following sections, we describe the architecture responsible for the collection and integration of data, which can be seen as a PCS horizontal operator.

III. Data Integration Architecture

A. Semantic Integration

The proposed here solution to heterogeneous data collection and integration is based on a Triple Space [3] as the approach to implementing an open interconnected system. A triple space is a special case of a tuple space. A tuple space is an implementation of an associative memory (also known as blackboard or distributed shared memory) for parallel or distributed computing. A repository of tuples (ordered lists of data elements) is provided that can be accessed concurrently; producers post their data as tuples in the space and consumers retrieve data from the space using queries or a subscription mechanism. In result, most of the direct communication between system components is substituted with posting to and reading from the tuple space. Such an approach separates the data themselves from such questions as data availability (where to find it?) and transmission (when and where to send?), thus greatly simplifying distributed application development. This paradigm has become quite popular in the Internet of Things field with many storage and integration Cloud services, such as Xively (formerly Cosm and before that Pachube), being such tuple spaces.

Semantic technologies based on machine-interpretable representation formalism have shown promise for describing objects, sharing and integrating information, and inferring new knowledge [10]. Therefore, [10] states that utilisation of semantic technologies is important for interoperability, data integration, data abstraction and access, resource search and discovery as well as reasoning and interpretation on the Internet of Things. Also, [1] argued for semantics in a wider context of PCS systems (see Section I).

Merging the tuple space paradigm with semantics, the result is a triple space where all the tuples are semantic triples {subject, predicate, object}. Some proprietary triple-space-based approaches were developed, including generic, such as [3], and specifically with resource-limited devices in mind, such as Smart-M3 [11]. However, with the present state of the technology, a triple space can also be set up without any proprietary software – via deploying an off-the-shelf RDF data server and posting and reading data using the standard SPARQL language and protocol.

In our solution, we followed the latter approach of relying on standards and reliable data storage products. In particular, we utilise an OpenRDF Sesame database deployed on an Apache Tomcat HTTP server. Data producers interact with various sensors using the special protocols that those sensors support and publish the observations to a Sesame repository as RDF triple-sets (see below). Data consumers never interact with data producers directly and only look for needed observations to appear in the database. Data prosumers, again, do not interact with any data producers or consumers directly, but read data from the database and output their results back into the database. All of these communications occur over the interface offered by the database which is SPARQL 1.1 Protocol over HTTP with SPARQL 1.1 Query or SPARQL 1.1 Update payloads. To facilitate data producer/consumer programming, we developed, however, software libraries (Java and C) hiding the HTTP and SPARQL operations and offering a simple to use programmatic API.

One drawback of using an off-the-shelf RDF database instead of a proprietary triple space solution is that subscriptions with push-notifications are not available to data consumers – a mechanism typically included into proprietary systems [3], [11]. A subscription mechanism offers two main advantages: (1) more convenient client programming and (2) avoiding the database and the network load with frequent repeated queries, or introducing a delay to reacting to new data. To address the latter and more important issue, our solution includes a *Change Notifier* service, which is a simple Web service (Java servlet) deployed on the same Tomcat instance as the Sesame database. It operates based on the ’long-polling’ model. This means that, after receiving a request, it waits for up to the specified timeout before responding with a response indicating that that no change occurred in the database. If any change occurs in the database during the waiting time, the service will immediately return and provide the timestamp of the change. One may use also ’since’ request parameter with a timestamp. This simple service allows avoiding unnecessary repetition of queries, as well as executing a query immediately after some new data become available, providing close to real time reaction as often required in Internet of Things environments.

The conceptual data model of our solution is principally based on the W3C’s SSN Ontology [4]. The SSN ontology is a domain-independent ontology that describes sensors and observations by merging sensor-focused, observation-focused and system-focused views. SSN is based itself on the DUL (DOLCE Ultra Light), with DOLCE standing for Descriptive Ontology for Linguistic and Cognitive Engineering. DUL is an upper ontology that defines only 5 classes at the top level of the concepts hierarchy, Object, Quality, Event, Abstract, and InformationRealization, as well as a larger set of properties for describing possible relationships between instances of these classes and their subclasses. Most of the concepts defined in SSN are then subclasses, sub-properties, or other derivatives of DUL concepts.

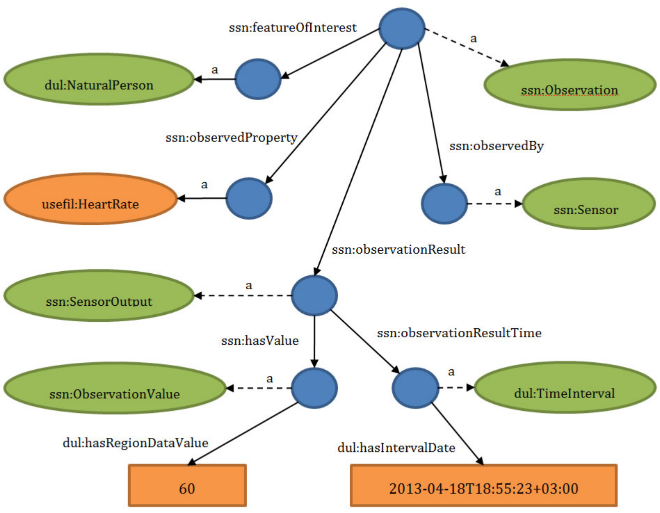


Fig. 1. An example of the description of a sensor observation.

Following SSN, we conceptually describe a sensor observation as depicted in Figure 1. Practically, we define and use, however, a more compact representation which reduces the number of triples and introduces only one anonymous node per measurement instead of seven in Figure 1 (blue circles). This is done without losing semantics via use of the OWL2 property-chain mechanism. In terms of Figure 1, every important path from the root to a leaf is substituted with a single custom property. For example, *usefil:observationResult* is defined as owl:propertyChainAxiom (ssn:observationResult ssn:hasValue dul:hasRegionDataValue).

With respect to required domain-specific concepts, such as types of observations (usefil:HeartRate in Figure 1, not covered by SSN or DUL), our approach is to either use concepts from established domain ontologies or to define custom concepts as subclasses of those. In the case of the USEFIL system, we utilised such ontologies as International Classification of Functioning, Disability and Health (ICF), International Classification of Diseases (ICD-10), SNOMED Clinical Terms, and Clinical Measurement Ontology (CMO).

B. *Tasker Framework*

To support automated management of a triple space, we have defined and implemented a software tool we refer to as the *Tasker framework*. Tasker allows timed and repeated execution of various SPARQL tasks on an RDF database, as well as execution of external Java code. It can be used as a library or a stand-alone application, in both cases controlled fully via its configuration file. Such a configuration file is encoded using Turtle RDF and contains definitions of one or more tasks. An example of a task follows.

```
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix t: <http://www.vtt.fi/usefil/tasker#> .
[a t:Task]
    t:prefixes ”PREFIX usefil: <http://usefil.eu/ontology#>” ;
    t:where ”?event usefil:observationResultTimeMillis ?time.
      FILTER (?time < %NOW% - 3600000). ?event ?p ?o” ;
    t:delete ”?event ?p ?o” ;
    t:construct ”?event ?p ?o” ;
    t:execute ”fi.vtt.usefil.tasker.executable.Backup” ;
    t:start ”12:00” ;
    t:repeat ”600000” ;
    rdfs:comment ”Remove old events” .
```

Each task is a *t:Task* instance and can have the following properties (all of which are optional):

- *rdfs:comment* Name of the task.
- *t:enabled* If false, the task is inactive.
- *t:prefixes* Task-specific SPARQL prefixes (other than rdf:, rdfs:, owl:).
- *t:where* Corresponds to WHERE clause of SPARQL. Used in a SELECT query and/or INSERT, DELETE, CONSTRUCT queries.
- *t:insert* Corresponds to INSERT clause of SPARQL.
- *t:delete* Corresponds to DELETE clause of SPARQL.
- *t:construct* Corresponds to CONSTRUCT clause of SPARQL.
- *t:execute* A Java class name, optionally followed by command line arguments, to be dynamically loaded and

executed. This class has to implement a predefined interface through which Tasker will feed it the results of execution of SELECT and/or CONSTRUCT queries.

- *t:start* Start time (first run) for the task. Can be an ISO 8601 time (e.g., 2013-11-10T12:00:00+0200) or a number in milliseconds which is interpreted as delay from the initialization time. Also partial forms of ISO 8601 time are accepted, like 12:00 above (which assumes current date and local time zone).
- *t:repeat* Repetition interval for the task, in milliseconds. Additional values are 0 meaning execution only once and -1 meaning execution every time a change occurs in the database (see Section III-A about Change Notifier).

The above example task thus removes from the database all the observations older than one hour (3600000 ms), while backing them up as RDF into a file (the *Backup* executable does that for the CONSTRUCT query result). This task is executed every 10 minutes (600000 ms) starting at noon.

Using different combinations of the task properties, Tasker can achieve a variety of goals, including data management (as in the example), rule-based reasoning / data fusion, as well context-dependent execution of application code.

C. Secutity Aspects

Along with the design of the above data integration architecture, an extensive analysis was performed of its security properties. Threats and vulnerabilities related to different security domains [12] were listed and addressed via specific measures. This analysis is outside the scope of this paper; below we only list the most prominent aspects.

The database server has to enforce secure communication, i.e., HTTPS, even if only used within a wireless network protected using WLAN security. This is to authenticate the server to data producers/consumers to prevent client spoofing by a fake server, as well as to prevent wireless eavesdropping among connected devices. The server also has to require the clients to authenticate for both data access and publication. This protects data from unauthorised access and prevents database spoofing, where a malicious software process publishes fake observations. Specifically, we register each data producer separately (own username and password) and insert any triples it submits into a separate sub-graph of the database, facilitating provenance tracking and non-repudiation. Data producers have to be designed to only push measurements to the database and not to implement any own query interfaces that would require a separate protection, which may be difficult. Finally, all the clients have to avoid storing any private data into temporary local files, i.e., should rely only on the database for persistence.

IV. Collecting Human Observations

A. Management of a Machine-Human Dialog

In the context of the general architecture described in Section III, collecting human self-observations is an issue of design of a specific type of a data producer.

Systematic collection and processing of human observations in general has been a rapidly growing topic in the research community. In particular, may studies address citizen sensor networks [5], which refer to interconnected networks of people who actively observe, report, collect, analyze, and disseminate information via text, audio, or video messages. These approaches focus on the analysis of readily-available *unsolicited* observation streams, in particular from microblogging systems such as Twitter. In contrast, we are interested in *solicited* observations, such as self-observations of a personal state. For solicited observation, Web-based online questionnaire forms remain a dominant tool, while there seems to be no streamlined approach to integration of answers from such online forms with physical sensor measurements.

In our solution, a questionnaire is defined as a state-machine and encoded in an XML document. In addition to messages, questions and answer options, this document includes all the information needed for the interpretation of answers in terms of our conceptual data model as well as accessing data from the triple space to personalise the questions. A state-machine representation allows two ways of administering a questionnaire. For longer questionnaires, we automatically transform them into Web forms. For shorter questioning sessions, we are also able to administer them question-by-question via an instant messaging protocol. For the latter case, we implemented both text-based and speech-based interfaces. For the text-based option, we developed a custom Android chat app that renders the answer options as buttons in the chat window (Figure 3). The use of a standard XMPP chat client is also possible, except for that the answers have to be typed then.

Figure 2 provides an example of a questionnaire definition that encodes the first question from Beck Depression Inventory (BDI) and is accompanied by a preamble and a closing message.

A questionnaire consists of *d:Message* and *d:Question* elements, the order of which is defined via their *d:state* and *d:transition* attributes. Upon a message, transition to the new state is done immediately. Upon a question, the transition is done only after a valid answer is received. The starting state is called ”start” and the final one ”end”. While a message only has *d:Text* property (the message itself), a question also has to have: *usefil:observedProperty*, which is the type of observation collected with this question, and a set of possible answers to the question. Each *d:Answer* has:

- *d:Text*. Text to display.
- *d:Value*. Identifier of the answer option, e.g., ”0”. If the user interface does not show answer options as list or buttons, but requires typing or speaking, values are used as accepted entries.
- *d:Shortcut* (optional). Another accepted entry corresponding to the answer option, e.g., ”no”.
- *usefil:observationResult*. Value for the evaluated usefil:observedProperty if this answer is selected.
- *d:Message* (optional). A message to deliver back to the user as a feedback to the answer.

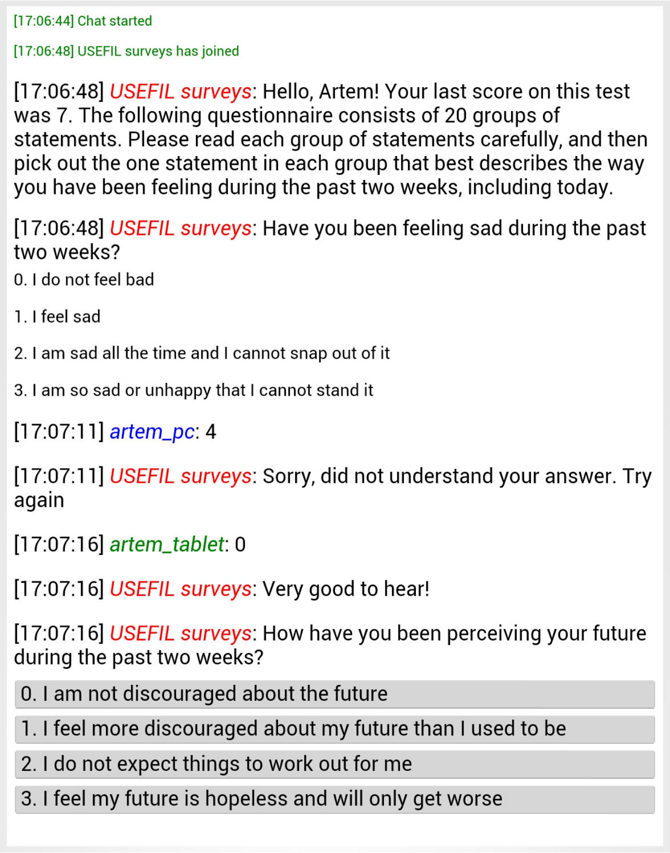
```
<d:Questionnaire xmlns:usefil=”http://usefil.eu/ontology#”
    xmlns:d=”http://usefil.eu/dialog#”
    xmlns:db=”http://usefil.eu/database#” id=”BDI” >

  <d:Message d:state=”start” d:transition=”1”>
    <db:Query db:type=”sparql”><![CDATA[
      PREFIX usefil: <http://usefil.eu/ontology#>
      SELECT * WHERE {
        [a usefil:User] usefil:hasName ?name .
        [a usefil:Measurement]
          usefil:observedProperty usefil:BDI;
          usefil:observationResult ?beck_score }
    ]]></db:Query>
    <d:Text>
      Hello, %name%! Your last score on this test was
      %beck_score%. The following questionnaire consists of ...
    </d:Text>
  </d:Message>

  <d:Question d:state=”1” d:transition=”2”>
    <d:Text>Have you been feeling sad
        during the past two weeks?</d:Text>
    <usefil:observedProperty>usefil:FeelingSad
        </usefil:observedProperty>
    <d:Answer d:transition=”3”>
      <d:Shortcut>no</d:Shortcut>
      <d:Text>0. I do not feel bad</d:Text>
      <d:Value>0</d:Value>
      <usefil:observationResult>0.0</usefil:observationResult>
      <d:Message>
        <d:Text>Very good to hear!</d:Text>
      </d:Message>
    </d:Answer>
    <d:Answer> ... <d:Answer>
    ...
  </d:Question>

  <d:Question d:state=”2”> ... </d:Question>
  ...
  <d:Message d:state=”21” d:transition=”end”>
    <d:Text>Thank you for your answers!</d:Text>
  </d:Message>

</d:Questionnaire>
```

Fig. 2. The questionnaire definition format.

- *d:transition* attribute (optional). Overrides that on the question, e.g., answering ”no” to the example question will lead to skipping the next question.

Any Message or Question can also have an optional *db:Query* property, giving a query that has to be executed on the triple space prior to delivery of the message/question. The values retrieved for the query variables will substitute corresponding placeholders in *d:Text* content.

Our implementation of the instant messaging approach is based on the XMPP messaging protocol. A user can have a number of user interface devices connected simultaneously; in USEFIL, this includes Smart TV, tablet, wrist-wearable unit, and a speech interface (on a PC). A question is received and rendered on all currently connected devices and can be answered from any of them. In USEFIL, we plan to use the instant messaging approach not only for soliciting health-related self-observations, but also in a number of other tasks. This includes validation of systems interpretations (”do you need to call somebody for help?”, ”does your wrist unit have to be charged?”) or to collect feedback (”was it easy to use the application?”).



[17:06:44] Chat started

[17:06:48] USEFIL surveys has joined

[17:06:48] USEFIL surveys: Hello, Artem! Your last score on this test was 7. The following questionnaire consists of 20 groups of statements. Please read each group of statements carefully, and then pick out the one statement in each group that best describes the way you have been feeling during the past two weeks, including today.

[17:06:48] USEFIL surveys: Have you been feeling sad during the past two weeks?

0. I do not feel bad

1. I feel sad

2. I am sad all the time and I cannot snap out of it

3. I am so sad or unhappy that I cannot stand it

[17:07:11] artem_pc: 4

[17:07:11] USEFIL surveys: Sorry, did not understand your answer. Try again

[17:07:16] artem_tablet: 0

[17:07:16] USEFIL surveys: Very good to hear!

[17:07:16] USEFIL surveys: How have you been perceiving your future during the past two weeks?

0. I am not discouraged about the future

1. I feel more discouraged about my future than I used to be

2. I do not expect things to work out for me

3. I feel my future is hopeless and will only get worse

Fig. 3. An example of a questionnaire chat session.

B. Speech Interface

A number of studies [9], [13] argued that, especially in the case of an ICT system assisting elderly persons, the use of speech-based interfaces is beneficial and may increase the end user acceptability of the system.

The text-to-speech transformation needed for a message/question delivery is a simpler problem supported by a number of reliable tools. Speech recognition, on the other hand, is shown to be a particularly hard problem to be solved reliably for most environments. Our approach to collecting self-observations, however, presents a very restricted case of the general speech recognition problem. First, in our case, only the machine can initiate the dialog by posing a question. Therefore, we do not face a hard problem of interpreting a free-form user command, which is a case for most speech-based systems. Second, the vocabulary that the user is expected to use when answering a question is predefined and very limited. In our XML format, the answering vocabulary for a question is the union of *d:Value* and *d:Shortcut* properties of all defined answer options. For the example question is Section IV-A, such vocabulary consists of eight words ’0’, ’1’, ’2’, ’3’, ’no’, ’yes’, ’always’, and ’unbearably’. Speech recognition in the case of such a very limited vocabulary is shown to be a much simpler and manageable problem.

We implemented a speech interface as an XMPP client, which thus can be used along with text-based XMPP clients. Any message/question received from the system is translated to speech using Mary TTS system. User’s answer is recognised using Simons Listens system and, if it is deemed to belong to the acceptable vocabulary, translated into XMPP and sent back to the system. Simon Listens supports dynamically restricting the expected vocabulary, providing a sufficient performance level in an indoor environment.

V. Conclusions

In this paper, we introduced a software architecture aiming to provide one required horizontal operator for Physical-Cyber-Social systems that is the collection and semantic integration of physical sensor measurements and human-produced observations, in particular, self-observations. While triple-space based data integration is an established approach, our architecture relies on standard protocols and reliable data storage products, which is an advantage compared to most existing solutions.

We believe, however, that the central contribution of this work lies with its approach to systematic collection of human observations via instant messaging. To the best of our knowledge, this has not been implemented before. Beyond collecting health-related self-observations, as in USEFIL, this approach can be utilized in a variety of other applications including citizen sensing, opinion polling, and feedback collection. Compared to Web survey forms, an instant messaging based survey (via a smartphone) has a number of advantages. Questions can be asked ”while they are hot” and conveniently responded with just one touch, questions can be personalized, questions that are asked (or not asked) next may depend on answers given to previous questions, as well as there is an option of a seamless handover from, e.g., a PC to a mobile device during a questioning session. An expected result is a higher response rate and a higher accuracy of responses.

Although the focus of this paper is on data collection and integration, as it is in PCS studies, the proposed architecture is grounded in an even wider view of [14], [15], which one of the authors of this paper co-originated. While PCS focuses predominantly on observing, i.e., sensing, [14] argued for a need to address the *device-software-human triangle* in a way allowing each of the three worlds to perform any of the basic computing functions: sensing, actuating, processing, and control. While focusing in this paper on the integration of machine sensing with human sensing, our architecture equally allows the integration of physical actuating with human actuating (e.g., sending a message to a person with a request to switch off unnecessary lights), software processing with human processing (e.g., sending a message to a person asking to translate a term), and software control with human control (e.g., providing a person with a list of possible courses of action and asking to select one).

In USEFIL, the work in 2014 includes conducting several-month-long pilot studies in Greece, UK, and Israel with real elderly subjects at their own homes. These pilots will provide a performance and usability evaluation of the system described in this paper as well as of other USEFIL products. Beyond USEFIL, our future work plans focus on further development and exploitation of the instant messaging survey approach in other applications. Some of these applications, e.g., feedback collection, are mentioned above.

Acknowledgements

This work is performed in the EU FP7 project USEFIL: Unobtrusive Smart Environments for Independent Living (Grant Agreement 288532).

References

[1] A. Sheth, P. Anantharam, and C. Henson, “Physical-cyber-social computing: An early 21st century approach,” IEEE Intelligent Systems, vol. 28, no. 1, 2013, pp. 78–82.

[2] A. P. Sheth, P. Barnaghi, M. Strohmaier, R. Jain, and S. Staab, “Physical-Cyber-Social Computing (Dagstuhl seminar 13402),” Dagstuhl Reports, vol. 3, no. 9, 2014, pp. 245–263.

[3] K. Teymourian, L. J. B. Nixon, D. Wutke, R. Krummenacher, and H. Moritsch, “Implementation of a novel semantic web middleware approach based on triplespaces,” in Proc. Intl. Conf. Semantic Computing, 2008, pp. 518–523.

[4] M. Compton et al., “The SSN ontology of the W3C semantic sensor network incubator group,” J. Web Semantics, vol. 17, 2012, pp. 25–32.

[5] A. Sheth, “Citizen sensing, social signals, and enriching human experience,” IEEE Internet Computing, vol. 13, no. 4, 2009, pp. 87–92.

[6] E. I. Papageorgiou, A. S. Billis, C. A. Frantzidis, E. I. Konstantinidis, and P. D. Bamidis, “A preliminary fuzzy cognitive map - based desicion support tool for geriatric depression assessment,” in Proc. IEEE Intl. Conf. Fuzzy Systems, 2013, pp. 1–8.

[7] N. Katzouris, A. Artikis, F. Makedon, V. Karkaletsis, and G. Paliouras, “Event recognition for assisted independent living,” in Proc. 6th Intl. Conf. Pervasive Technologies Related to Assistive Environments. ACM, 2013, pp. 26:1–26:5.

[8] C. Cannuscio, J. Block, and I. Kawachi, “Social capital and successful aging: The role of senior housing,” Annals of Internal Medicine, vol. 139, no. 5 part 2, 2003, pp. 395–399.

[9] P. Wu and C. Miller, “Results from a field study: The need for an emotional relationship between the elderly and their assistive technologies,” in Proc. Intl. Conf. Augmented Cognition, 2005.

[10] P. M. Barnaghi, W. Wang, C. A. Henson, and K. Taylor, “Semantics for the internet of things: Early progress and back to the future,” Int. J. Semantic Web and Information Systems, vol. 8, no. 1, 2012, pp. 1–21.

[11] J. Honkola, H. Laine, R. Brown, and I. Oliver, “Cross-domain interoperability: A case study,” in Proc. Conf. Smart Spaces (ruSMART), LNCS 5764, 2009, pp. 22–31.

[12] R. Savola and M. Sihvonen, “Metrics driven security management framework for e-health digital ecosystem focusing on chronic diseases,” in Proc. Intl. Conf. Management of Emergent Digital EcoSystems, 2012, pp. 75–79.

[13] F. Portet, M. Vacher, C. Golanski, C. Roux, and B. Meillon, “Design and evaluation of a smart home voice interface for the elderly: acceptability and objection aspects,” Personal and Ubiquitous Computing, vol. 17, no. 1, 2013, pp. 127–144.

[14] A. Katasonov, O. Kaykova, O. Khriyenko, S. Nikitin, and V. Y. Terziyan, “Smart semantic middleware for the internet of things,” in Proc. 5th Intl. Conf. Informatics in Control, Automation and Robotics, 2008, pp. 169–178.

[15] V. Terziyan, A. Katasonov, J. Cardoso, M. Hauswirth, and A. Majumdar, “PRIME: Proactive inter-middleware for global enterprise resource integration,” Eastern-European Journal of Enterprise Technologies, vol. 51, no. 3/12, 2011, pp. 3–16.

Acceptance of Mobile Payment Service Designs in Complex Ecosystems

Pergler, Elisabeth
CAMPUS 02 University of Applied Sciences, Information Technologies & Business Informatics,
Graz, Austria
e-mail:
elisabeth.pergler@campus02.at

Adelsberger, Christian
Glatz, Daniela
evolaris next level GmbH,
Graz, Austria
e-mail:
christian.adelsberger@evolaris.net;
daniela.glatz@evolaris.net

Schamberger, Rainer
PSA Payment Services Austria GmbH
Vienna, Austria
e-mail: rainer.schamberger@psa.at

***Abstract*—This paper presents the results of an acceptance analysis of existing mobile payment services (MPS) and MPS concepts. The analysis was conducted by means of technical documentation on features and functionalities, usage tests and interviews with experts from the MPS ecosystem. The results indicate high acceptance of wallet MPS that support additional functionalities such as loyalty card inclusion. In addition, card-based MPS obtain high values for ease of use, and thus, might serve as transitional solution until technical standards are implemented in the ecosystem. Subsequent to a short introduction and presentation of the state of the art, the development of the evaluation framework of this study will be presented on which the analysis of the MPS at hand is based. The paper concludes with the design of a field study that will evaluate the acceptance of the suggested MPS in a real-world context.**

Keywords-mobile payment service; technology acceptance; external factors; complex ecosystem

I. INTRODUCTION

Recent market research indicates a growing importance of mobile payment. At the beginning of 2013, Gartner [1] predicted that the value of the mobile payment transactions will increase by 44 percent in 2013 compared to 2012, to an estimated $235.4 billion worldwide by the end of the year.

In some regions, such as Japan and the US, mobile payment is already part of people’s everyday lives. The development on the European markets, on the other hand, is still behind prior expectations. There exists high insecurity among many potential stakeholders within the complex ecosystem of mobile payment. The insecurity refers to technology standards as well as service designs and business models.

What makes the ecosystem of different MPS "complex" is the fact that different pre-conditions and circumstances are relevant for each solution. Some examples include relevant partners in the value creation/delivery and supply chain process, a variety of contract forms, agreements, legal aspects, and responsibilities. For the user of a single MPS this complex ecosystem means that they might not be able to use the chosen MPS for the payment at a certain retailer, because the involved parties and companies are not in a contractual relationship that is necessary for a successful transaction at the point of sale.

Acceptance of mobile payment is an issue that has been addressed in various empirical studies. These resulted in interesting causal models of mobile payment acceptance with high explanatory power, e.g., [2], [3], and [4]. Acceptance by itself, defined as the decision to adopt or not adopt a MPS, is not sufficient to predict the market success of a particular payment service as their success is highly dependent on the ecosystem in which they operate and their actual design. Thus, there is a need to connect theoretical foundations from acceptance research to practical design issues of actual mobile payment services and to context factors that arise from the complex ecosystem in which mobile payment services operate.

The main objective of the present research project is therefore a systematic analysis of generic mobile payment services (MPS) within a novel acceptance evaluation framework that is derived from validated causal models of mobile payment acceptance. In a first step, it is necessary to develop the evaluation framework based on an extensive literature review. Mobile payment services are classified based on a market analysis and representative services are selected for each generic service. These are then analysed within the acceptance evaluation framework. Data for the analysis is obtained from service features and mobile payment service usage tests and expert interviews with service providers, banking and payment experts. The comparison of acceptance factors for each service results in a systematic assessment and enables conclusions regarding acceptance of the analysed mobile payment services. The paper concludes with an outlook on a subsequent field study. The research design of the field study is based on the major findings of the presented project and is necessary to evaluate the results of this research project in a real world context.

The paper is structured as follows: Section II presents the state of the art. In Section III, we describe how the evaluation framework was developed, which is the basis for the analysis of different payment services (Section IV). The paper concludes in Section V, with an outlook to our future work and study design.

II. STATE OF THE ART

Analysis of the state of the art will start with Section A, in which the technological implementations of mobile payment services will be presented, followed by Section B,

ISBN: 978-1-61208-324-7

which will provide an introduction to the acceptance factors of mobile payment services.

A. Technological implementations of mobile payment services

Mobile payment services can be classified according to technological designs and features that influence the payment process. The following classification is based on [5] and [6]:

- carrier medium,
- payment method,
- technology,
- type of payment system,
- payment process, and
- storage of sensitive customer data.

Mobile payment services are differentiated according to the carrier medium that is used. In this study, smart phones and Near Field Communication (NFC)-cards are considered as media types. The second criterion is payment method. Possible types are debit as well as credit cards, pre-paid mechanisms and direct debit processes. Debit card payment either initiates account debiting immediately after the transaction at the point of sale or a couple of days later. Credit card payment does not initiate immediate debiting of the account, but enables a loan without interest for the rest of the month. The amounts of several transactions are accumulated and account debiting takes place at the end of each month. Pre-paid payment requires money to be deposited on a card or smart phone in advance. The payment method is accepted at the point of sale as long as the account balance is positive.

An important issue is the technology that is used to communicate with the payment terminal at the point of sale. Common technologies are NFC, 2D-codes and bar codes. Payment systems operate either in form of so called open-loop systems or closed-loop systems. Closed-loop systems involve one single bank that processes the transactions whereas open-loop systems involve several banks in the transaction process. Payment processes are either offline or online. Online payment processes require input of a PIN by the user at the terminal. This is necessary for identification of the card holder. The card is checked online and the transaction will be completed only after successful verification. Offline payment, on the other hand, does not include verification of the available payment limit at the bank in charge of the account. There is no identification and card verification at the point of sale and communication takes place only between smart phone or card and the terminal. There exist four main types of sensitive customer data storage. The construction-wise inclusion of the secure element embedded in the smart phone is one technical option. A major disadvantage of this type is the connection of the secure element and its data to a particular phone that cannot be transferred to another device. Another option is usage of micro-SD cards that are equipped with a secure element. These can be put in the micro-SD slot of the smart phone and transferred in case of device changes. The secure element can also be stored on the SIM card. As these are bound to a certain mobile network operator this might hamper changes of the mobile network operator. The fourth option is storage of sensitive customer data on a card that is equipped with an NFC chip.

B. Acceptance factors of mobile payment services

Many acceptance research studies of mobile payment acceptance are based on technology acceptance model (TAM) [7], and thus, incorporate perceived usefulness (PU) and perceived ease of use (PEOU) as main factors influencing behavioral intention (BI) to use, e.g., [8], [9], [10], etc. A comparative study in different cultural settings [8] included technology readiness as a personality trait in the original TAM. Results of this study indicate a significant positive effect of technology readiness on PEOU and PU as well as BI in most cultural settings. Individual mobility as a personal requirement regarding technology characteristics and perceived security resulted in positive effects on BI or attitude towards mobile payment in [4]. Personal innovativeness is another personality factor that has been tested with significant positive effects within the TAM framework [10]. This study also included technology characteristics such as convenience and reachability that showed positive effects on either PEOU or PU.

Security is one of the most often tested technology characteristics. In most cases, it is operationalized as a perception of security [4]. It has also been empirically tested in the particular setting of mobile payment acceptance in tourism [11]. In some studies, security issues are regarded as aspects of perceived risk and operationalized within this construct [9] and [12].

Trust is a construct that obtained particular interest within mobile payment acceptance research. Trust has been tested as an antecedent of PEOU and PU [3] and it has been found that it is affected by characteristics of the mobile technology itself and characteristics of the service provider, such as reputation. An examination of trust within the valence framework indicated highly dynamic effects of trust in internet payment and initial trust in mobile payment on negative valences (perceived cost and risk) and positive valence (relative advantage) that is affecting BI [2].

Other studies are based on unified theory of acceptance and use of technology (UTAUT) [13] and include social influence and other constructs in addition to PU and PEOU to explain BI. In [14], UTAUT was extended by the mobile payment specific factors trust and perceived security. Both factors resulted in significant effects on intention to use mobile wallets in the research model.

Contextual issues have been included in various studies in different forms. We apply the multidisciplinary context model from [15] in order to classify these constructs and variables in a systematic way.

- Social context refers to people around the subject, their relationships to the subject, and interactions with the subject. Social context includes, for example, subjective norm [4], reference group evaluation [12], friends' evaluation [12], etc.

- Task context considers the particular objective of the present usage situation. It is interpreted [16] as a breadth of mobile payment use situations [12] or circumstances in use situations.
- Physical context includes all objects that are surrounding the subject and their current status and direction. Examples for the inclusion are the construct individual mobility [4] and compatibility [17], [2].
- Temporal context is what gives the current usage situation a meaning like, e.g., past mobile payment use [12].

Value is a neglected factor in empirical research on mobile payment acceptance but is included in a theoretical model of mobile wallet adoption that has been applied in a case study [18]. N. Guhr et al. [8] define perceived value as “a trade-off between what customers receive, such as quality, benefits, and utilities, and what they sacrifice, such as price, opportunity cost, transaction cost, time and efforts” [18]. Finance-related risks, such as perceived costs, did not show significant effects on BI in an empirical study on acceptance of a card-based payment service [9]. A study on consumers’ willingness to pay for mobile payment services indicated that consumers are either not willing to pay any fee for using mobile payment or the fee varies between different purchased goods [16]. Value is not only important in the context of user acceptance but also in the bigger context of the eco-system. Cost for the bank server and security as technology quality were included in an analytic hierarchy process and turned out to be important factors within the context of technological mobile payment decisions [19].

III. Development of Evaluation Framework

In this chapter, the evaluation framework will be described. First, an overview to the Evaluation Process (Section A) will be provided, followed by the selection of acceptance factors in Section B. These factors will be operationalized in Section C.

A. *Evaluation Process*

The evaluation is illustrated in Figure 1 (Sequence Diagram Evaluation Process). It shows that the process was based on the identification of relevant acceptance factors through literature review. These factors were operationalized and applied to all selected MPS by the means of usage tests and expert interviews. MPS were selected based on a thorough desk research, in which all information and data available were collected. Further and deeper information was gathered through usage tests and expert interviews. As a result, for each MPS and each of the relevant acceptance factors, a classification was suggested, whether the potential of acceptance of the MPS at hand is to be considered high, medium, or low. The evaluation process was carried out from February to August 2013.

This classification was based on a discussion process within the project team and double-checked by external MPS experts. Usability tests were not part of the analysis, as it can be assumed that this aspect will be covered in time before market launch of the MPS.

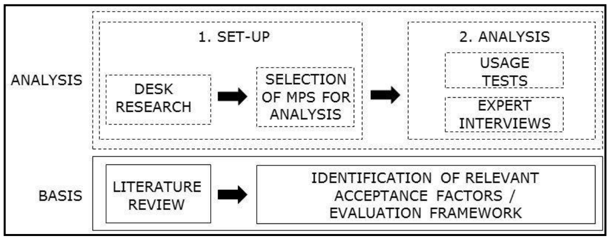

ANALYSIS
1. SET-UP
DESK RESEARCH
SELECTION OF MPS FOR ANALYSIS
2. ANALYSIS
USAGE TESTS
EXPERT INTERVIEWS
BASIS
LITERATURE REVIEW
IDENTIFICATION OF RELEVANT ACCEPTANCE FACTORS / EVALUATION FRAMEWORK

Figure 1. Sequence Diagram Evaluation Process

B. *Selecting acceptance factors*

Acceptance factors for the evaluation framework are derived from the literature review. PEOU and PU are the most widely used constructs to explain acceptance of mobile payment. Their concepts are provided in Table 1.

TABLE I. Perceived ease of use / Perceived Usefulness

Acceptance Factor	***Construct***	***Definition***
Perceived Ease of Use	PEOU [9], [11], [10], [8], [14]	The original definition from [7] “the extent to which using a new system is expected to be free of efforts”
	PEOU [4]	“Important aspects related to mobile payment services ease of use include, for example, clear symbols and function keys, few and simple payment process steps, graphic display, and help functions […]”
Perceived Usefulnes	PU [9], [11], [10], [8], [14]	The original definition from [7] “the degree to which a prospective adopter believes that by using a particular system would improve his or her job performance”
	Attitude [12]	“This construct can be taken to reflect an individual’s attitude towards a MPS, ranging from a very positive to a very negative assessment of the system’s utility.”
	PU [4]	“[…] users are only willing to accept innovations if those innovations provide a unique advantage compared to existing solutions […]”
	Convenience [10]	“Convenience is nothing but a combination of time and place utilities, which are clearly principal characteristics of m-payment.”

Trust, perceived risks and (perceived) security were also included in many studies. Table 2 lists the various tested concepts.

TABLE II. SECURITY-RELATED FACTORS

Construct	***Definition***
Perceived risk [2]	"[…] extent to which prospective users expect mobile payment services to be uncertain or risky."
Initial mobile payment trust [2]	"Trust is a subjective belief that a party will fulfill his or her obligations according to the expectations of the trusting party."
Perceived risk [9]	"[…] the expectation of losses related to purchase […]"
Perceived security [11]	"[…] a threat which creates circumstance, condition or event with the potential to cause economic hardship […]"
MPS risk [12]	"The MPS risk construct refers to the possible harmful consequences an individual expects from MPS use […]"
Consumer trust [3]	"[…] in the context of m-payments, the two dimensions of consumer trust are trust in mobile service provider and trust in technology facilitated by mobile service provider characteristics and mobile technology characteristics respectively."
Perceived environmental risk [3]	"[…] is the risk associated with the underlying technological infrastructure […]"
Perceived structural assurance [3]	"[…] the consumer's perception about the institutional environment […]
Perceived security [4]	"In the context of electronic services, security risk, conceptualized as the likelihood of privacy invasion, has been found to be a particularly critical concern […]"
Perceived security [14]	"[…] the degree to which a customer believes that using a particular mobile payment procedure will be secure."
Trust [14]	"[…] the belief that vendors will perform some activity in accordance with customers' expectations."

External factors, such as necessary hardware or software adaptations, are included in the analysis due to their influence on provider decisions whereas other factors, such as availability and provider characteristics, are excluded from this analysis as these are highly influenced by time and location of assessment, e.g., Google wallet is currently not available in Austria but might be in future. Personal character traits and social influence are also excluded for this analysis as they are strictly individual but will be included in a future field study. The same is true for the different concepts of value which will be in the focus of the field study.

C. Operationalization of acceptance factors

In a next step, the four major constructs were operationalized in order to obtain measures for mobile payment service usage tests and issues for the expert interviews. These methods were necessary, as detailed desk research on the technical features and functionalities was only partly able to cover the complexity of the topic at hand and usage tests were only possible for existing MPS. Details and functionalities regarding conceptualized MPS were obtained from interviews.

The process of operationalization focused on mobile payment procedures and features of different services.

Ease of use is analyzed considering the steps a user needs to take before using the mobile payment service and the process of each transaction. Moreover, some additional processes are considered such as PIN changes and payment history or analysis features.

Usefulness is analyzed with regard to transaction speed, i.e., average time that is required per transaction, considering quicker transactions as more useful. Also, additional functionalities are examined, such as integration of loyalty cards or shop finder.

Security is analyzed considering storage of sensitive customer data and risks that occur in operation.

External factors that affect the ecosystem are considered in terms of required adaptations at the bank and point of sale in order to enable the MPS to operate.

IV. ANALYSIS OF MOBILE PAYMENT SYSTEMS

Ten different existing mobile payment services and feasible mobile payment concepts were included in the analysis. They cover different combinations of technical implementations and designs. As a limitation, it has to be stated that the selection of MPS is based on desk research and the project team's understanding of the most possible combinations of technology and designs, no study or literature exists in this regard to suggest a different mode of selection:

1. NFC debit card in an open-loop system enabling online and offline payments (e.g. PSA Payment Services Austria GmbH with all Austrian banks)
2. NFC pre-paid card in a closed-loop system enabling offline payments (e.g. Quick by PayLife)
3. NFC credit card in an open-loop system enabling online and offline payments (e.g. Mastercard PayPass and Visa PayWave)
4. Debit/credit application for smart phones with additional NFC hardware in an open-loop system enabling online and offline payments (e.g. CardMobile)
5. Barcode debit application for smart phones in an open-loop system enabling online payments (e.g. Secure Payment Technologies GmbH - pilot test)
6. Account-based 2D-code application for smart phone in an open-loop system enabling online and offline payments (e.g. CellumPay)
7. NFC debit/credit wallet application for smart phone in an open-loop system enabling online payments (e.g. Google Wallet)
8. NFC credit wallet application for smart phone in an open-loop system enabling online payments (e.g. myWallet by German Telekom)
9. 2D-code debit/credit application for smart phone in a closed-loop system enabling online payments (e.g. Starbucks and Square)
10. NFC debit application for smart phone in an open-loop system enabling online and offline payments (concept only)

Table 3 provides an overview on relevant factors for assessing ease of use, taking into account aspects before usage, the process of transaction and additional aspects.

With regard to the required effort of users before usage and during each transaction, card-based MPS are most easy to use. Wallet applications are also easy to use and in most cases offer additional functionalities like in-application PIN changes that increase ease of use. Barcode-based MPS are least easy to use as they require additional activities in the course of each transaction process.

TABLE III. ANALYSIS OF EASE OF USE

MPS	*before usage*	*transactions*	*other aspects*
1	Existing card is replaced by NFC enabled card; no registration required	Amount appears on terminal display; card is put close to display; visual or audio signal; NFC chip information is read by terminal; card is removed; successful transaction indicated by visual or audio signal; random PIN requests	PIN is changed at the bank; no history or analysis available
2	Existing card is replaced by NFC enabled card; no registration required; top up money	Amount appears on terminal display; card is put close to display; visual or audio signal; NFC chip information is read by terminal; card is removed; successful transaction indicated by visual or audio signal; amount is debited immediately from prepaid account	No PIN; application for smart phone that reads NFC chip and provides transaction history and account balance
3	Existing card is replaced by NFC enabled card; no registration required; one contact payment required	Amount appears on terminal display; card is put close to display; visual or audio signal; NFC chip information is read by terminal; card is removed; successful transaction indicated by visual or audio signal; random PIN requests	No history or analysis available
4	Download iOS 5.0 or higher and application; additional hardware for iPhone; registration of card; top up money	Application is launched; smart phone is put close to display; visual or audio signal; amount is displayed; amounts from 20 Euro require individual passcode; transaction is confirmed	PIN can be changed via application; transaction history for 30 days and account balance
5	Online banking activation; application download; application and account activation via transaction number and activation number;	Application is launched; PIN authorization; payment code is provided; barcode on smart phone display is scanned at the terminal; transaction is verified online	PIN can be changed anytime
6	Application download; registration of application via text message; creation of mobile PIN; registr. credit card; activation of credit card	Phone number and payment ID are provided to cashier; cashier selects payment method; customer receives confirmation request; card is selected; PIN is entered; confirmation is sent as push notification; cashier receives confirmation	PIN can be changed via application; transaction history available;
7	Application download; account registration; activation of credit card; test transaction	Application is launched; smart phone is put close to display; payment information is transferred automatically; transaction is confirmed by customer	PIN can be changed via application; transaction history and payment analysis via Google account
8	Application download; replace existing SIM card by myWallet NFC SIM card; registration	Application is launched; login information is entered; customer selects card; smart phone is put close to display; transaction is initiated; amounts from 25 Euro require PIN	PIN can be changed anytime; transaction history available
9	Application download; card registration	Pay by square: Application is launched; card is selected and QR code appears; cashier scans QR code; invoice is sent via email Pay by face: application is launched; name and photo are assigned using GPS information; cashier confirms matching face and photo	PIN can be changed via application; transaction history and analysis available
10	no details available	no details available	no details available

Usefulness (see Table 4) ought to be highest for wallet solutions as they include additional functionalities. The same is true for code-based MPS, but there is no information available regarding transaction speed of these services. Card-based MPS are considered to be very fast considering transaction speed, and thus, increase user perceptions of usefulness but do not enable any additional functionalities.

TABLE IV. ANALYSIS OF USEFULNESS

MPS	*transaction speed*	*additional functionalities*
1	offline payment (up to 25 Euros) approximately 350 milliseconds; online payment takes longer as it requires a PIN	none
2	200 – 300 milliseconds at POS terminal; 500 milliseconds at ATM	none
3	approximately 1 second without PIN;	none
4	online payment approximately 1 second; offline payment less than 1 second	none
5	no details available	none
6	online approximately 4 to 7 seconds	loyalty card inclusion; sweepstakes; prepaid card handling; mobile ticketing; mobile commerce inclusion
7	depends on payment situation	personalization features; Google offers inclusion
8	no details available	individual daily transaction limits; loyalty card inclusion
9	no details available	shop finder; invoice via email
10	no details available	no details available

Security issues, which are analyzed in Table 5, are rather balanced among MPS except for stored value technologies.

These might cause actual loss of money for the customer. Storage of sensitive customer data can influence ease of use as mobile phone and mobile network operator respectively are not easy to change in case of embedded secure elements or SIM-based secure elements. Transaction limits increase security, but may also harm ease of use and, in some cases, even usefulness, e.g., when transactions are made impossible. A similar effect is caused by PIN requirements. They increase security of the MPS but decrease ease of use and transaction speed.

TABLE V. ANALYSIS OF SECURITY

MPS	*storage of sensitive data*	*countermeasures against risks in operation*
1	on NFC chip on the card	random PIN requests (after five transactions the latest) for low value transactions; PIN required for transactions from € 25s
2	on NFC chip on the card	stored value technology is a risk considering theft as money is stored on the card with no further authorization required
3	on NFC chip on the card	random PIN requests (after four transactions the latest) for low value transactions; PIN or signature required for transactions from 25 Euros
4	secure element on MicroSD	only service provider can access secure element; additional app login possible; stored value is limited to € 50
5	none	barcodes are valid only once and only for 4 minutes; limit of 10 transactions per day; limit of € 100 per day; limit of 4 payments per hour
6	data is split between smart phone and remote server	mobile PIN for each transaction; remote deactivation of application available
7	embedded secure element and Google Cloud	remote deactivation available; transaction limit of $1.000 per day for one device and $10.000 for more than one device
8	SIM-based secure element	data encryption on NFC-SIM; card and smart phone can be locked; individual daily limits
9	not applicable	online deactivation of application available; pay by face: face authentication
10	SIM-based secure element	certificates to avoid fraud

Table 6 provides an overview of the relevant external factors for MPS analysis. Considering the point of sale, most MPS require adaptations with regard to terminals and software. Some are based on cash desk software adaptations as well. The most intrusive MPS design (number 6) even requires a connection between the point of sale and the remote server of the MPS provider. Effects on participating banks are minor to those on participating retailers. Those that require adaptations of the bank-wise core system are less likely to succeed unless initiated by the bank.

TABLE VI. ANALYSIS OF EXTERNAL FACTORS

MPS	*bank*	*point of sale*
1	adaptations in backend system required	NFC terminals and software required; no changes with regard to business processes and interchange fee model
2	none	NFC terminals and software required; no changes with regard to business processes and interchange fee model
3	none	NFC terminals required; no changes with regard to software, business processes and interchange fee model
4	none	NFC terminals required; particular module for low value transactions required; no changes with regard to business processes and interchange fee model;
5	adaptation of core system required	particular barcode scanner required (smart phone display scan enabled); cash desk software required; no interchange fee
6	none	connection of point of sale system to backend system and remote server; QR code printer or display required; no interchange fee
7	none	NFC terminals required
8	none	NFC terminals required; no changes with regard to business processes and interchange fee model;
9	none	QR code reader required; display required; adaptation of network, terminal and software infrastructure; acceleration of business processes (order, payment); no interchange fee
10	mobile issuing infrastructure including mobile network operators and banks required	NFC terminals required; no changes with regard to business processes and interchange fee model

V. CONCLUSION AND OUTLOOK ON FUTURE WORK (FIELD STUDY DESIGN)

Table 7 presents the results of the analysis, that indicate high potential of acceptance for NFC-based wallet MPS (number 7 and 8) and NFC card-based MPS (number 1, 2 and 10). Face verification did obtain optimistic results in the analysis, but requires very intrusive external adaptations, and, moreover, does not support open-loop payment systems. Whereas high ease of use and high usefulness are positive indicators of overall acceptance, the effects of security on ease of use and usefulness can be either positive or negative.

TABLE VII. RESULTS ANALYSIS

MPS		*ease of use*	*usefulness*	*security*	*security → EOU*	*security → U*
1		high	medium	medium	negative	negative
2		high	medium	low	positive	positive
3		high	medium	medium	negative	negative
4		medium	medium	low	none	none
5		medium	?	medium	negative	negative
6		low	medium	high	negative	none
7		high	high	high	none	none
8		medium	high	medium	negative	none
9	Pay by face	high	high	high	positive	none
	Pay by square	medium	high	medium	none	none
10		?	?	medium	negative	none

In the field study design, card-based solutions will be tested against wallet MPS according to the obtained analysis results, taking the complex eco-system of mobile payment solutions into consideration. Therefore, a central aim of the field study will be the identification of those factors that add specific value to mobile payment and how these factors could be implemented successfully. “Success” will not only be measured by the extent of technology acceptance, but also by the extent to which the solutions are suitable for different personalities, use situations, social constellations etc., hence, taking a variety of context factors into account. The main research questions are:

- What kind of differences with regard to acceptance can be identified between card-based solutions and MPS?
- Are there acceptance differences between transaction types (debit vs. credit)?
- Differences could be stated regarding relative benefits, perception of value, perceived complexity, security, trustworthiness, and consequences of PIN requirements and the like.
- Which MPS is believed to be most successful (wisdom of crowds)?
- How is the concept of “wallet” perceived and rated and what are customers’ associations and demands in this regard?
- Are there any influences/changes on daily routines expected? What kind of influences/changes are there? Are they the same for all MPS?

In order to tackle this huge variety of research questions and also taking the complex eco-system of MPS into account, the field study will consist of three parts, each applying different methods. In a field trial, 70 respondents will use two card-based solutions (debit, credit) and two mobile-phone-based MPS (debit, credit) over a period of two to three months complementing their common payment methods and provide feedback continually via standardized questionnaires, before, during and after the survey period. In addition in situ feedback will be provided via mobile questionnaire after each purchase. In total, each participant will be using MPS between eight and ten times at least, using each solution at least once.

After the trial, a small number of participants will be invited to take part in a co-creation session in order to further optimize the identified most promising MPS and also in order to explore possible consequences for their daily lives.

Besides the users’ point-of-view, the experiences and perspectives of the major stakeholders in the MPS eco-system providing the test-setting (financial institute, acquirers, issuers, and retailers) will be thoroughly analysed by means of expert interviews.

ACKNOWLEDGMENT

This research project is funded within COMET (Competence Centers for Excellent Technologies) program.

REFERENCES

[1] S. Shen, “Forecast: Mobile Payment, Worldwide, 2013 Update”, 2013.

[2] Y. Lu, S. Yang, P. Y. K. Chau, Y. Cao, „Dynamics between the trust transfer process and intention to use mobile payment services: a cross-environment perspective,“ Information & Management, vol. 48, 2011, pp. 393-403.

[3] S. Chandra, S. C. Sristava, and Y.-L. Theng, “Evaluating the role of trust in consumer adoption of mobile payment systems: an empirical analysis,” Communications of the Association for Information Systems, vol. 27, 2010, Article 29, pp. 561-588.

[4] P. G. Schierz, O. Schilke, and B. W. Wirtz, „Understanding consumer acceptance of mobile payment services, an empirical analysis,“ Electronic Commerce Research and Applications, vol. 9, 2010, pp. 209-216.

[5] C. Neger, “ Types of cashles payment in Austria. Plastic money,” (=Varianten des bargeldlosen Zahlungsverkehrs in Österreich. Plastikgeld), 2010, VDM, Saarbrücken.

[6] M. Verdier, “Retail payment systems: what can we learn from two-sided markets?,” Communication & Strategies, vol. 61, 2006, pp. 37-56.

[7] F. D. Davis, “ Perceived usefulness, perceived ease of use and user acceptance of information technology, “ MIS Quarterly, vol. 13, 1998, pp. 319-339.

[8] N. Guhr, T. Loi, R. Wiegard, and M. H. Breitner, „Technology readiness in customers’ perception and acceptance of m(obile)-payment: an empirical study in Finnland, Germany, the USA and Japan,” Proceedings of the 11th International Conference on Wirtschaftsinformatik, 27th February – 1st March 2013, Leipzig, Germany, pp. 119-133.

[9] G. W.-H. Tan, K.-B. Ooi, S.-C. Chong, and T.S. Hew, “NFC mobile credit card: the next frontier of mobile payment?,” Telematics and Informatics, in press, 2013.

[10] C. Kim, M. Mirusmonov, and I. Lee, “An empirical examination of factors influencing the intention to use mobile payment,” Computers in Human Behavior, vol. 26, 2010, pp. 310-322.

[11] R. Peng, L. Xiong, and Z. Yang, “Exploring tourist adoption of tourism mobile payment: an empirical analysis,” Journal of

Theoretical and Applied Electronic Commerce Research, vol. 7, 2012, pp. 21-33.

[12] T. J. Gerpott and K. Kornmeier, “Determinants of customer acceptance of mobile payment systems,” International Journal of Electronic Finance, vol. 3, 2009, pp. 1-30.

[13] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, “User acceptance of information technology: toward a unified view,” MIS Quarterly, vol. 27, 2003, pp. 425-478.

[14] D.-H. Shin, “Towards an understanding of the consumer acceptance of mobile wallet,” Computers in Human Behavior, vol. 25, 2009, pp. 1343-1354.

[15] N. A. Bradley and M. D. Dunlop, “ Toward a multidisciplinary model of context to support context-aware computing,” Human-Computer Interaction, vol. 20, 2005, pp. 403-446.

[16] D. Viehland and R. S. Y. Leong, „Consumer willingness to use and pay for mobile payment services,” International Journal of Prionciples and Applications of Information Science and Technology, vol. 3, 2010, pp. 35-46.

[17] C. Li and M. Zhang, “Research on the factors affecting consumers’ willingness to the use of mobile payment,” in Advances in D. Zheng (Ed.): Computer Science and Engineering, ASIC 141, pp. 575-580.

[18] D. L. Amoroso and R. Magnier-Watanabe, “Building a research model for mobile wallet consumer adoption: the case of Mobile Suica in Japan,” Journal of Theoretical and Applied Electronic Commerce Research, vol. 7, 2012, pp. 94-110.

[19] A. Sanayei and A. Ansari, “Selection of the appropriate mobile payment technology in mobile banking, “ International Journal of Information Science and Management, Special Issue 2, 2010, pp. 13-26.

Regional Information Platform and Information Distribution System in Telecommunication and Broadcasting Convergence

~For Tourism Promotion and Disaster Prevention~

Tadashi Miyosawa, Hiroo Hirose,
Takeshi Tsuchiya
Department of Business Administration and Information
Tokyo University of Science, Suwa
Chino, Japan
{miyosawa, tsuchiya.takeshi, hirose}@rs.suwa.tus.ac.jp

Hideyasu Karasawa, Hidenaga Karasawa
Data Cake Baker Corporation
Tama, Japan
{hideyasu.karasawa,hidenaga.karasawa}@dcb.co.jp

Wataru Kameyama
Global Information and Telecommunication Institute
Waseda University
Honjo, Japan
wataru@waseda.jp

Keiichi Koyanagi
Graduate School of Information, Production and Systems
Waseda University
Kitakyusyu, Japan
keiichi.koyanagi@waseda.jp

Hisashi Yamamoto
Chino Machidukuri Laboratory
Chino, Japan
yamamoto@chino.machiken.jp

Kenichi Masuzawa
Media Mix Group
LCV Corporation
Suwa, Japan
masuzawa.kenichi@lcv.co.jp

Abstract—**As the main focus of this research, we constructed an experimental website for the communication broadcasting cooperative transmission system and developed a regional information platform. In addition, we carried out a small-scale demonstration experiment at the Chino station. The results of the questionnaire show that there is high demand for the provision of regional information, as was initially expected. However, the level of satisfaction regarding the kind of information people wanted was higher with one-segment (1Seg) transmission. It appears that 1Seg is better at sorting and presenting information believed to be necessary, and that there are comparatively few people who want in-depth information unique to particular regions such as that provided by social network services. This means that the system should dynamically change the ratio of general and in-depth information based on the time, location, and user profile.**

Keywords-regional information; disaster prevention; tourism promotion; crawling; 1Seg

I. INTRODUCTION

In March 2012, the Japanese Tourism Agency adopted the new "Tourism Destination Promotion General Plan" as a basic plan to transform Japan into a tourism-oriented country. The authorities considered expanding tourist locations and improving the quality of tourism as the main directions for the plan. Specific goals were set, with the aim of increasing domestic travel spending to 30 trillion yen by 2016 and the number of foreign travelers to 18,000,000, while also improving traveler satisfaction. Tourism is one pillar of the growth strategy for Japan, and is also contributing to the recovery effort relating to the Great East Japan Earthquake [1].

Furthermore, the Japanese Tourism Agency is evaluating the need for a "Tourism Regional Development Platform" and has made these documents publicly available [2]. Regional tourism development is shifting from an organized group travel model to an individual or small group model, while participatory experience-type travel needs are growing, and travelers' needs are diversifying. To address these changes in travel needs and to establish networking projects to attract visitors, various concerned parties at the destinations need to meet and cooperate in a cross-sectional and substantive manner that will develop local tourism, by utilizing resources and offering products and services (optional tourism type products) unique to each region. Simply having concerned parties provide local travel products in their respective specialty fields, however, is not enough to carry out marketing that will determine what products are in demand, and tends to be insufficient as a system for dealing with complaints. Thus, in order to not only utilize local resources and sell local travel products, but also promote regional economic development that can sell these products and services, a regional tourism development platform providing a one-stop information center for selling local travel products across the sectors is a necessity.

The area around Chino is blessed with a rich variety of natural tourism resources such as Tateshina Plateau and the Yatsugatake Mountains, and is host to many tourists. Recently, however, a decline in travelers has led to a decline in spending, creating a serious problem. The lack of coordination between tourism operators has been raised as an issue in tourism recovery. Since Chino is a popular location for tourism, many tourism companies operate there; however, because most of these operators promote their activities individually, the effect is not a consolidated one. This is why there is a demand for a centralized "receptacle" organization to be established, which could manage operations and advertising for all customers under a united banner [3]. Thus, the "Tourism Regional Development Platform" is indeed a necessity.

Considering disaster prevention information, a wide range of information needs to be covered, including weather and river information, which is transmitted by each region, as well as earthquake information. As each type of information is transmitted through different media and in different formats, it is not possible to consolidate everything. In addition, manually converting media and formats means that information cannot be transmitted in real-time, and thus a system structure capable of immediate transmission is needed.

It is also apparent from experiences with the Great East Japan Earthquake that society depends on mobile phone networks, the Internet, and other digital information transmission infrastructure. Besides the use of social media and e-mail in times of emergency to confirm a person's safety, frequent access to websites via mobile phones and 1Seg public information broadcasts were also recorded.

In other words, the Great East Japan Earthquake proved that the various means of broadcasting and Internet communication complimented each other, and in so doing, confirmed the need to secure an information transmission system that can distribute information in a variety of formats.

One channel in Japan's terrestrial digital broadcasting format (ISDB-T) is split into thirteen sections, called "segments." A few of these segments are bundled together to send video, data, and audio. One of these segments, called one-segment (1Seg), is used exclusively for broadcasting to mobile devices. 1Seg local services in Japan are broadcasts aimed at mobile devices, although the service is limited to a few small regions.

Until now, the 1Seg local service broadcast was an experimental service, utilizing unused bands of the television broadcasting spectrum (white space). Various experiments were carried out in each community and service as a place ("special white space zone") to conduct research and development in addition to verification tests for the institutionalization of new services and systems as well as for business development and promotion. Expectations are high for the application thereof, especially in the fields of regional tourism recovery and disaster prevention.

This paper consists of an introduction in Section 1, and a discussion of past research in Section 2. Section 3 explains the aims of this research at a conceptual level. Section 4 discusses the implementation of the research and experiments, while Section 5 gives the details and results of the experiments. Finally, Section 6 presents a summary and discusses options for future research.

II. Past Research

To the best of our knowledge, there are no examples of previous hands-on studies that have comprehensively addressed local area information systems and information transmission systems, as this research aims to do. The following examples are provided as related research.

There have been several reports on 1Seg local service experiments including those by Saito et al. [5] on tests conducted at the Sapporo Snow Festival, and Nishikawa [6]. In addition, numerous reports exist on experiments carried out on the transmission of information using 1Seg local services. There are also examples in which 1Seg has been used to tackle actual tasks in local areas.

Research on basic technology for data mining has resulted in advancements, and the effectiveness thereof is expected to improve. Deguchi [7] suggested the possibility of content navigation through recommendation and data mining. Additionally, Haseyama and Hisamitsu [8] investigated the use of video searching technology to allow users to access a particular video from among a great number of videos.

Prompted by the Association for the Promotion of Public Local Information and Communication, the work in [9] attempted to further standardize area information platforms from the viewpoint of municipalities.

In 2008, the Ministry of Internal Affairs and Communications established the Research Society for Regional Safety and Security Information Foundations, and proposed the construction of "safety and security public commons" [10], a mechanism to provide the foundation for sharing disaster information. From this, the "commons format XML" was established as a format for sharing information, which led to the creation of the "public information commons". Since June 2011, this service has been operating as an entity managed by the Foundation for MultiMedia Communications (FMMC). This paper uses the public information commons, and proposes a disaster prevention information transmission system.

In 2012, research was carried out on a regional information platform and 1Seg local broadcast service for tourism promotion and disaster prevention [11]. During the research, which contributed to the design of the fundamental concepts of the current research project, a 1Seg local service broadcasting experiment for a large-scale event (the Lake Suwa fireworks display) was carried out. And in the past research showed that through optimal use of communication and broadcasting, user's benefit was maximized [12].

III. Area Information Platform and Information Transmission System

This research is based on the conceptual design of one of the results from last year's research on the area information platform and information transmission system, and presents results based on tangible development and experimentation. In Section 3, the basic conceptual design is explained.

To transmit tourist and disaster prevention information in a timely fashion to those needing it, a regional information platform has been constructed. Development for data mining, content comprehension technology, and sampling technology amongst others, has also been carried out to gather and analyze the information, and then automatically generate and organize the information desired by the user. Transmission experiments were conducted to confirm the platform's effectiveness.

The current state is that tourism information for large areas is scattered, so the desired information cannot be obtained instantly. In addition, accessing individual or deep, hidden information is challenging. For these reasons, the regional information platform is designed to be included social media as illustrated in the lower portion of Fig. 1, and information on narrow region will be sourced through data mining. In addition, conceptually, as shown in the upper portion of the Fig. 1, a tourism and disaster prevention information transmission system that can link up with media from broadcasts or transmissions will be built. In terms of the transmitted content, the platform can connect with broadcasts and transmissions in a coordinated fashion, and can be optimized to organize programs according to the analysis of user data. An autonomous disaster prevention information system will also be created, to consider the possible use of broadcasts and transmissions in the event of a disaster.

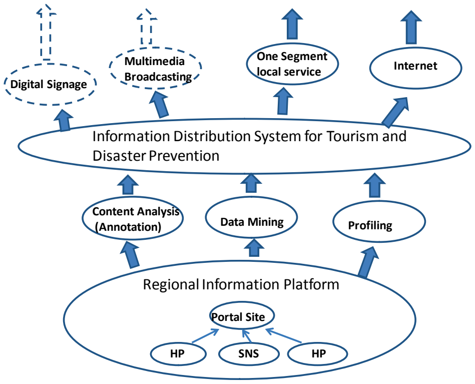

Digital Signage
Multimedia Broadcasting
One Segment local service
Internet
Information Distribution System for Tourism and Disaster Prevention
Content Analysis (Annotation)
Data Mining
Profiling
Regional Information Platform
Portal Site
HP
SNS
HP

Figure 1. Regional information and distribution system

Whereas our previous research focused on a 1Seg local service broadcast transmission experiment at a large-scale event (the fireworks show), the transmission experiment in this research sets out to investigate an area information platform system and transmission system with the ability to link with broadcasts and transmissions.

IV. System Implementation

A. Overall Construction

Fig. 2 shows the overall system configuration. The upper part of Fig. 2 corresponds to the area information platform shown in Fig. 1, while the lower part corresponds to the information transmission system.

The Regional Tourism Information Database crawls web sites, blogs, and other online resources of local individuals transmitting information, allocates weights to the detected keywords according to frequency, and stores them in a database. In addition, the Area Disaster Prevention Information Database regularly polls public information commons [10], not only gathering the latest information from the commons, but also detecting other information, such as the region's torrential rain information.

To report disaster prevention information in a timely manner on a tourism and disaster prevention portal site, work is underway to transfer such information from the Disaster Prevention Information Database to the Tourism Information Database, thereby allowing disaster prevention warning information to be presented without delay on the portal site.

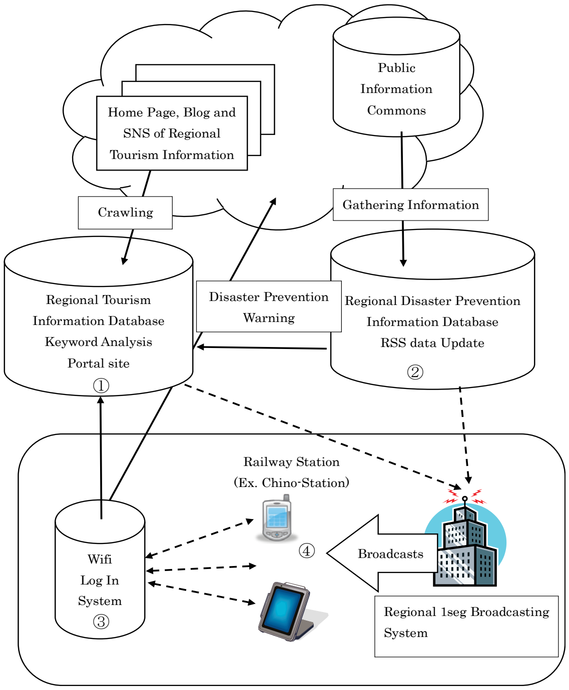
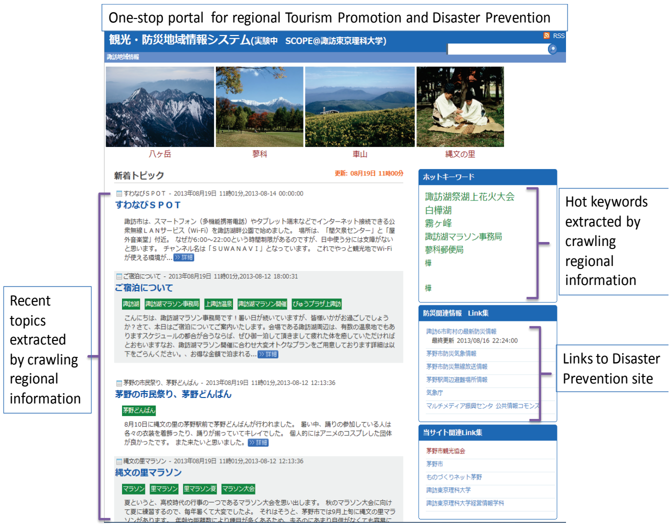

Home Page, Blog and SNS of Regional Tourism Information
Public Information Commons
Crawling
Gathering Information
Regional Tourism Information Database Keyword Analysis Portal site
①
Disaster Prevention Warning
Regional Disaster Prevention Information Database RSS data Update
②
Railway Station (Ex. Chino-Station)
Wifi Log In System
③
④
Broadcasts
Regional 1seg Broadcasting System

Figure 2. System configuration

B. Area Information Platform and Portal Site Construction

This corresponds to the part of Fig. 2 demarcated as ①. A platform has been created that can centrally manage not only official local area websites, but also personal sites, blogs, and social networking services (SNS), amongst others. By creating a one-stop portal site such as this, users (tourists) will be able to find the information they seek without having to search several sites. Additionally, local knowledge of the region can be extracted by crawling regional information, which is then analyzed according to what users want, and is uploaded to the portal site illustrated in Fig. 3. Moreover, we believe that this can be reflected in 1Seg broadcast programs.

Several of the existing tourist websites, such as those for the various tourist associations, hot springs associations, tourist operators, and special event committees were analyzed by the web crawler system which is installed in Tokyo University of Science, Suwa. A crawler program is used to search for keywords related to the Suwa region; the resulting website data is imported and analyzed with the results shown in Fig. 3. This effectively creates the one-stop portal for regional information. Dealing with information that is transmitted only by SNS, for example, information on the local Tateshina Plateau vegetable market, which was scheduled to be held every Sunday, but was suspended once owing to a typhoon, is not that simple; if you do not know the SNS address, you cannot view the information. However, if “Tateshina” is picked up as a keyword, a relationship is created from this keyword and it is possible to see the information.



One-stop portal for regional Tourism Promotion and Disaster Prevention

観光・防災地域情報システム(実験中　SCOPE@諏訪東京理科大学)

RSS

諏訪地域情報

八ヶ岳　蓼科　車山　縄文の里

新着トピック　更新: 08月19日 11時00分

すわなびＳＰＯＴ - 2013年08月19日 11時01分,2013-08-14 00:00:00

すわなびＳＰＯＴ

諏訪市は、スマートフォン（多機能携帯電話）やタブレット端末などでインターネット接続できる公衆無線ＬＡＮサービス（Wi-Fi）を諏訪湖畔公園で始めました。 場所は、「間欠泉センター」と「屋外音楽堂」付近。 なぜか6:00～22:00という時間制限があるのですが、日中使う分には支障がないと思います。 チャンネル名は「ＳＵＷＡＮＡＶＩ」となっています。 これでやっと観光地でWi-Fiが使える環境が... >> 詳細

ご宿泊について - 2013年08月19日 11時01分,2013-08-12 18:00:31

ご宿泊について

諏訪湖　諏訪湖マラソン事務局　上諏訪温泉　諏訪湖マラソン開催　びゅうプラザ上諏訪

こんにちは、諏訪湖マラソン事務局です！暑い日が続いていますが、皆様いかがお過ごしでしょうか？さて、本日はご宿泊についてご案内いたします。会場である諏訪湖周辺は、有数の温泉地でもありますスケジュールの都合が合うならば、ぜひ御一泊して頂きまして疲れた体を癒していただければとおもいますなお、諏訪湖マラソン開催に合わせ大変オトクなプランをご用意しております詳細は以下をごらんください。、お得な金額で泊まれる... >> 詳細

茅野の市民祭り、茅野どんばん - 2013年08月19日 11時01分,2013-08-12 12:13:36

茅野の市民祭り、茅野どんばん

茅野どんばん

8月10日に縄文の里の茅野駅前で茅野どんばんが行われました。 暑い中、踊りの参加している人は各々の衣装を着飾ったり、踊りが揃っていてキレイでした。 個人的にはアニメのコスプレした団体が良かったです。 また来たいと思いました。 >> 詳細

縄文の里マラソン - 2013年08月19日 11時01分,2013-08-12 12:13:36

縄文の里マラソン

マラソン　里マラソン　里マラソン夏　マラソン大会

夏というと、高校時代の行事の一つであるマラソン大会を思い出します。 秋のマラソン大会に向けて夏に練習するので、毎年暑くて大変でしたよ。 それはそうと、茅野市では9月上旬に縄文の里マラソンがあります。 年齢や距離数により種目が多くあるため、走るのにあまり自信がなくても容易に

ホットキーワード

諏訪湖祭湖上花火大会
白樺湖
霧ヶ峰
諏訪湖マラソン事務局
蓼科郵便局
樺
樺

防災関連情報　Link集

諏訪6市町村の最新防災情報
最終更新 2013/08/16 22:24:00
茅野市防災気象情報
茅野市防災無線放送情報
茅野駅周辺避難場所情報
気象庁
マルチメディア振興センタ 公共情報コモンズ

当サイト関連Link集

茅野市観光協会
茅野市
ものづくりネット茅野
諏訪東京理科大学
諏訪東京理科大学経営情報学科

Recent topics extracted by crawling regional information

Hot keywords extracted by crawling regional information

Links to Disaster Prevention site

Figure 3. One-stop regional portal site

C. *Development of an Autonomous Disaster Prevention Information System*

This section relates to the part of Fig. 2 demarcated by ②. When developing the autonomous disaster prevention information system, it was decided that the public information commons [10] would be used. The goals of this public information commons are: (1) to send quickly and accurately safety and security information that was transmitted to residents in regions with public institutions, such as local public bodies, to all residents using various types of media, (2) to transmit various media to residents by sending information only once to the commons, (3) to use a data format that has been standardized and unified, and (4) to provide the foundation for the distribution of shared information.

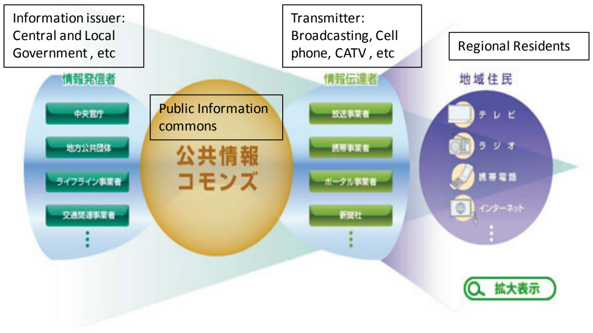
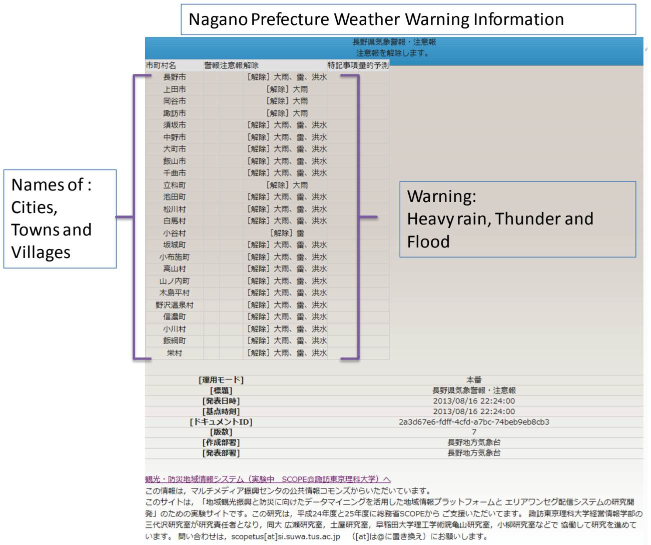


Figure 4. Public information commons conceptual design

Information originators positioned on the left of Fig. 4 are assumed to be central government agencies, local government, lifeline operators, and transportation related operators, for example. However, currently, almost all members are prefectural or municipal local governments. The majority of members that are information communicators, positioned on the right of Fig. 4, are local broadcasting offices, Cable television (CATV), Amplitude modulation (AM) / Frequency modulation (FM) radio, and community FM.

Extensible Markup Language (XML) format, which is used as a standardized data format, is versatile enough to express diverse and varied information under various conditions, from warnings and disaster information to peacetime activities. The public information commons is already being used to distribute evacuation advice/instructions, evacuation point information, emergency operation center establishment points, disaster information, events, notices, river water levels, rainfall information, early warning mail, weather and storm warnings, designated river water flood forecasts, and landslide alerts as actual information individually to several prefectures and cities.



Nagano Prefecture Weather Warning Information

長野県気象警報・注意報
注意報を解除します。

市町村名	警報	注意報	解除	特記事項	量的予測
長野市			［解除］大雨、雷、洪水		
上田市			［解除］大雨		
岡谷市			［解除］大雨		
諏訪市			［解除］大雨		
須坂市			［解除］大雨、雷、洪水		
中野市			［解除］大雨、雷、洪水		
大町市			［解除］大雨、雷、洪水		
飯山市			［解除］大雨、雷、洪水		
千曲市			［解除］大雨、雷、洪水		
立科町			［解除］大雨		
池田町			［解除］大雨、雷、洪水		
松川村			［解除］大雨、雷、洪水		
白馬村			［解除］大雨、雷、洪水		
小谷村			［解除］雷		
坂城町			［解除］大雨、雷、洪水		
小布施町			［解除］大雨、雷、洪水		
高山村			［解除］大雨、雷、洪水		
山ノ内町			［解除］大雨、雷、洪水		
木島平村			［解除］大雨、雷、洪水		
野沢温泉村			［解除］大雨、雷、洪水		
信濃町			［解除］大雨、雷、洪水		
小川村			［解除］大雨、雷、洪水		
飯綱町			［解除］大雨、雷、洪水		
栄村			［解除］大雨、雷、洪水		

[運用モード]	本番
[標題]	長野県気象警報・注意報
[発表日時]	2013/08/16 22:24:00
[基点時刻]	2013/08/16 22:24:00
[ドキュメントID]	2a3d67e6-fdff-4cfd-a7bc-74beb9eb8cb3
[版数]	7
[作成部署]	長野地方気象台
[発表部署]	長野地方気象台

観光・防災地域情報システム（実験中　SCOPE@諏訪東京理科大学）へ

この情報は，マルチメディア振興センタの公共情報コモンズからいただいています。
このサイトは，「地域観光振興と防災に向けたデータマイニングを活用した地域情報プラットフォームと エリアワンセグ配信システムの研究開発」のための実験サイトです。この研究は，平成24年度と25年度に総務省SCOPEから ご支援いただいてます。 諏訪東京理科大学経営情報学部の三代沢研究室が研究責任者となり，同大 広瀬研究室，土屋研究室，早稲田大学理工学術院亀山研究室，小柳研究室などで 協働して研究を進めています。 問い合わせは，scopetus[at]si.suwa.tus.ac.jp　（[at]は@に置き換え）にお願いします。

Names of : Cities, Towns and Villages

Warning: Heavy rain, Thunder and Flood

Figure 5. Screenshot during a Suwa region disaster alert

Fig. 5 shows an example of an actual heavy rainfall and flood warning released for the Suwa region. This type of warning is transmitted to the public information commons by the Nagano local meteorological observatory. The figure shows how it is presented on this regional information platform. Furthermore, from autumn 2013, Civil protection warning system in Japan (J-ALERT) is scheduled to be transmitted via the public information commons, and it is expected that almost all the safety and security information will be collated in the public information commons.

D. *Login System*

The Wireless Fidelity (WiFi) login system, which does not require prior registration, is illustrated in part ③ of Fig. 2. Tourism and disaster information is transmitted from this network interface. After logging in, the user enters the portal site as shown in Fig. 2, with disaster information also presented on this page. The login system consists of a WiFi transmission router and homepage, and a server for Dynamic Host Configuration Protocol (DHCP) control.

E. Construction of a Communication Broadcasting Cooperative Transmission System

This corresponds to the part demarcated as ④ in Fig. 2. By extracting data characteristics (mining), aspects such as the attention level and topics for a certain point in time and a certain location can be obtained, and dynamically formatted as a webpage matching the interests of the user. For broadcasting content, since program content is not directly and dynamically converted, it is possible to switch the display order for recommended locations based on the level of importance of the keyword about once a day. In the future, we intend accessing the Suwa tourism information database and converting the displayed content dynamically.

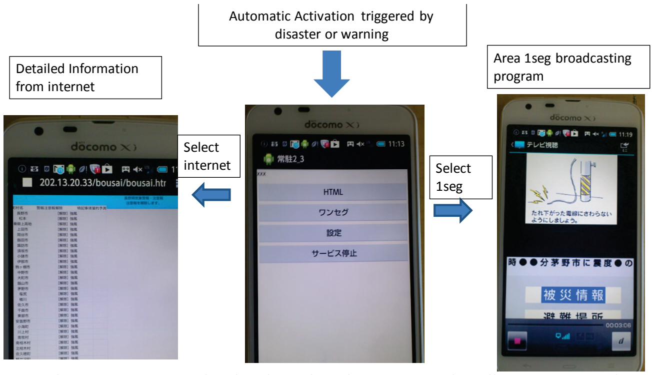

Automatic Activation triggered by disaster or warning
Detailed Information from internet
Area 1seg broadcasting program
Select internet
Select 1seg
docomo
202.13.20.33/bousai/bousai.htr
HTML
ワンセグ
設定
サービス停止
テレビ視聴
被災情報

Figure 6. Communication broadcasting cooperative disaster prevention operational screenshot

Furthermore, as shown in Fig. 6, when a disaster or a warning occurs, a permanently installed smartphone application detects events that occur thanks to the updates to the Disaster Prevention Information Database, which launches the disaster prevention application. When a disaster occurs, because the Internet and radio waves may not necessarily be available, it is possible to select whether to collect information from the Internet or 1Seg broadcast for the disaster prevention application. If the 1Seg broadcast is selected, the 1Seg function automatically starts, selects a disaster prevention broadcasting channel, and enables the user to watch certain programs such as immediate disaster prevention broadcasts, This function has been successfully implemented.

It is assumed that tourist programs will be shown by default, but that the system will switch to disaster prevention broadcasts if a disaster occurs.

V. TRANSMISSION AND BROADCAST-BASED EXPERIMENT AT CHINO STATION

Using the regional information platform that was developed, a communication broadcasting cooperative type transmission experiment was performed on August 21, 2013 at Chino station, as shown in Fig. 7.

During the experiment, information was transmitted to travelers who were waiting for trains to return home after visiting Chino for the summer vacation via 1Seg broadcasts using the Internet and weak radio waves. Every year at this time, 100 to 200 people are typically waiting for the limited number of express trains in the direction of Tokyo in waiting areas inside the station. We distributed a questionnaire to these people at 1 pm, just before the fireworks display was about to start, and collected their replies before 5 pm.

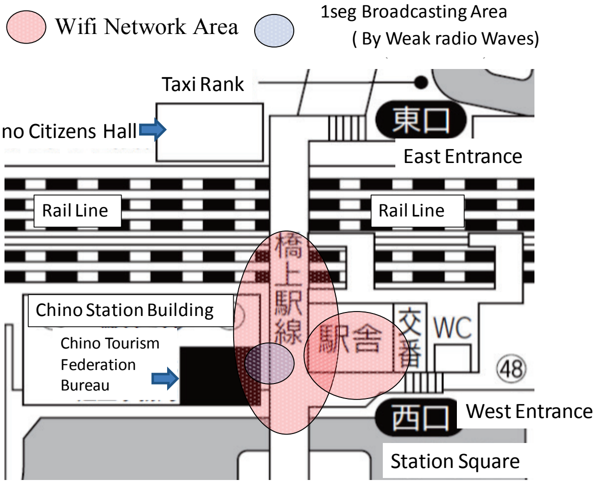


Figure 7. Experiment location: map of Chino station

A. Information Transmission System and Data Transmission using WiFi

For transmission using the Internet, a DHCP server and WiFi router were set up on the ceiling of a corridor on the second floor of the station. The tourism information database and disaster prevention information database servers were set up at the university. A public network connected these servers with the Chino station. Although several WiFi hotspots were already in operation within the station, the experiment required that the WiFi service be used without any prior registration, which meant that it should be possible to connect using only the Service Set Identifier (SSID) input. After connecting, as shown in Fig. 8, an image introducing tourism in Chino was displayed, which when clicked, was designed to connect directly to the tourist portal because the main goal of the WiFi service was for people to use the tourist portal and owing to the realization that a push type service was necessary.

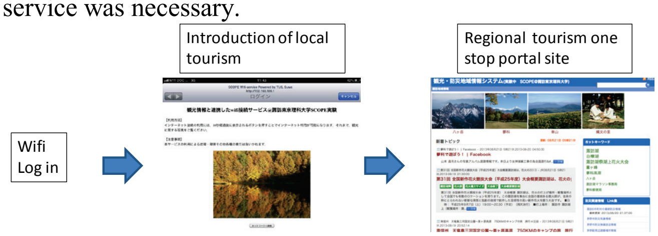

Introduction of local tourism
Regional tourism one stop portal site
Wifi Log in

Figure 8. Login screen and portal screen transition

B. Broadcast System using Weak Radio Waves

During the experiment content was transmitted using weak radio waves. A transmitting device for the experiment was placed around the tourist information area inside the station, and the experiment was performed within a range of several meters in which the transmissions could be received. The video content, which was pre-prepared Chino tourist and disaster prevention videos, was encoded by H.264, a video codec for 1Seg, saved on the device's hard disk drive, and repeatedly transmitted. In addition, a compilation of Broadcast Markup Language (BML) for the data broadcast section was created beforehand using authoring tools on a separate computer, stored on the device's hard disk drive, and repeatedly sent using a carousel method.

C. Broadcast Programs

The content for 1Seg was divided and displayed as videos at the top of the screen with the data broadcasting section at the bottom of the screen. The video section showed Chino tourist videos for standard tourism, and it was assumed that this would switch to disaster prevention videos during emergencies. During the experiment, to ensure the questionnaire was easy to complete, a tourist video was shown for approximately 3 min, while a disaster prevention video was shown for approximately 2 min. Both videos were shown repeatedly.

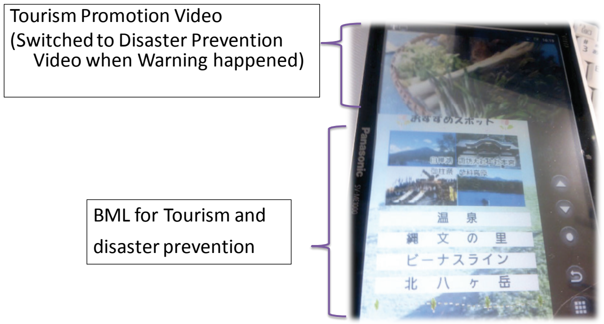

Tourism Promotion Video
(Switched to Disaster Prevention Video when Warning happened)
BML for Tourism and disaster prevention
おすすめスポット
温　泉
縄　文　の　里
ビーナスライン
北　八　ヶ　岳
Panasonic

Figure 9. Screenshot of 1Seg program on smartphone

Fig. 9 shows the smartphone program in use during the actual experiment. The top of the screen in this example displays a video introducing tourism in the Chino region, while the bottom of the screen displays text in the form of BML for tourists.

As shown in Fig. 10, information on a disaster and the prevention thereof can be acquired from the appropriate section on the display when a disaster occurs.

The regional information platform was accessed the day before the experiment to acquire tourist information. Keyword content relating the 1st to 4th ranking keywords is displayed in order with photos attached, while information relating to the 5th to 8th ranking keywords is displayed as large text entries. Additional items are displayed below this on the screen.

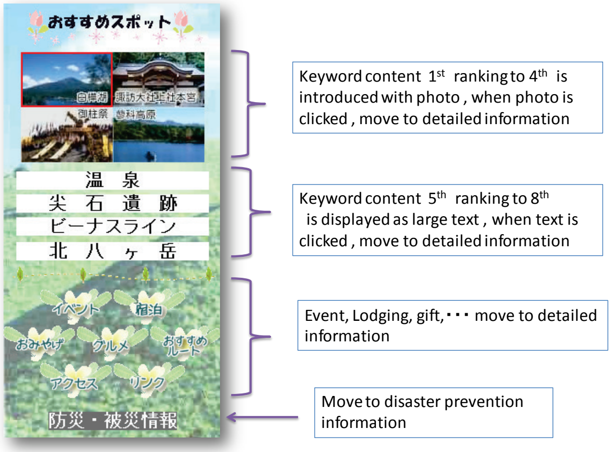
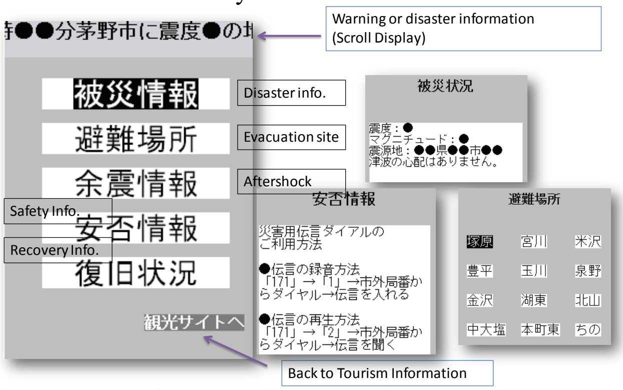

おすすめスポット
白樺湖
諏訪大社上社本宮
御柱祭
蓼科高原
温　泉
尖　石　遺　跡
ビーナスライン
北　八　ヶ　岳
イベント
宿泊
おみやげ
グルメ
おすすめルート
アクセス
リンク
防災・被災情報
Keyword content 1st ranking to 4th is introduced with photo , when photo is clicked , move to detailed information
Keyword content 5th ranking to 8th is displayed as large text , when text is clicked , move to detailed information
Event, Lodging, gift,・・・ move to detailed information
Move to disaster prevention information

Figure 10. Layout of smartphone screen

When selecting information on a disaster and the prevention thereof as shown in Fig. 11, the system is designed to confirm aspects like the state of the disaster, evacuation points, aftershock information, safety information, and the state of recovery.



時●●分茅野市に震度●の地

震度：●
マグニチュード：●
震源地：●●県●●市●●
津波の心配はありません。

災害用伝言ダイアルの
ご利用方法

●伝言の録音方法
「171」→「1」→市外局番か
らダイヤル→伝言を入れる

●伝言の再生方法
「171」→「2」→市外局番か
らダイヤル→伝言を聞く

Figure 11. Disaster prevention BML screen

D. Results and Considerations of the Questionnaire

Students from Tokyo University of Science, Suwa interviewed people in the vicinity of the tourist information kiosk in the Chino station as part of administering the questionnaire.

Information collected via the questionnaire includes:

- The kind of information users require
- Usefulness and evaluation of information obtained via the Internet
- Usefulness and evaluation of information obtained via 1Seg
- Comprehensive evaluation of information transmitted during the experiment
- Profile of the questionnaire respondents

While handing out the questionnaires, the students also explained the tourist portal and broadcast system in detail. As this took a great deal of time, about 40 min per respondent, questionnaires were only completed by 30 people, which was fewer than expected.

We used an evaluation scale from 0 to 4, with 4 being the best. Below we discuss the obtained results, where each figure is given as the average of the marks for all test subjects.

1) Questions about information required by users

The demand for information on tourist spots (3.60), access to transportation (3.57), weather forecasts (3.53), drinking and eating (3.47), accommodation (3.34), and recommended tourist routes (3.28) was high. In terms of disaster prevention information, there was high demand for information on the disaster itself (3.73) and evacuation points (3.60).

2) Usefulness and evaluation of information obtained via the Internet

Results of the questions evaluating information obtained via the Internet are shown in Fig. 12 and summarized below: usefulness (3.25), whether the correct information was found (2.89), whether the latest information was available (3.57), and whether the regional information was useful (3.57). It appears that information focusing on the region in particular was highly desirable.

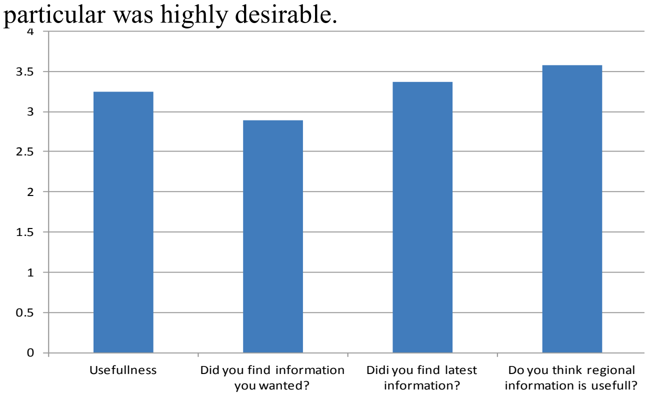


Figure 12. Usefulness and evaluation of information obtained via the Internet

Furthermore, when asking people to view and evaluate whether the content related to the top four keywords of the tourist portal via the Internet was useful, all items received an evaluation of 3 or above. This means that most of the test subjects agreed on the level of importance for the top keywords extracted by the system. Lake Suwa was ranked first, but we believe this is due to the many SNS articles about Lake Suwa, and the fact that during this time, many advertised events were due to take place at Lake Suwa.

In addition, for disaster prevention information, an average evaluation of 3.69 for the usefulness thereof was obtained, while the ability to view tourist and disaster prevention information on the same page received a high score of 3.72 on average.

3) Usefulness and evaluation of information obtained via 1Seg

Results of the usefulness of transmissions by 1Seg are shown in Fig. 13. High scores were received for access information (3.56), recommended routes (3.53), gourmet information (3.50), and hot springs guidance (3.47). Since test subjects were already at the Chino station, it appears that they were interested in return train access information and recommended routes for their next visit based on the individual tourist site information. The Togariishi archeological site (3.28) and tourist videos (3.21) were given low scores.

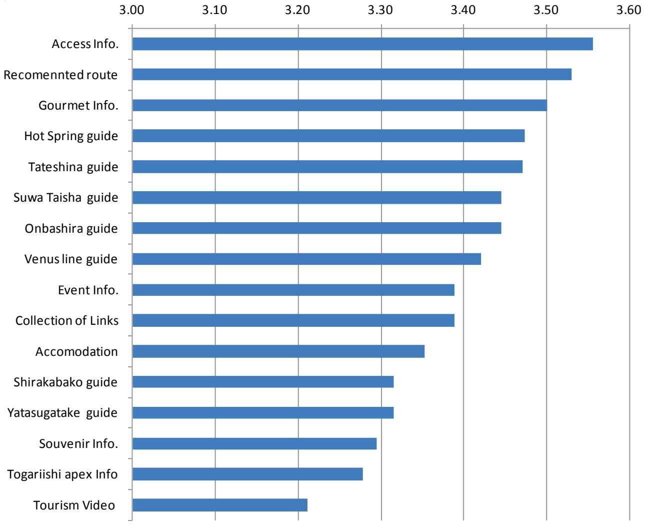


Figure 13. Usefulness of tourist information obtained via 1Seg

As shown in Fig. 14, regarding disaster prevention information, information allowing the user to decide what action to take following a direct disaster such as recovery information (3.72) and evacuation point information (3.63) was regarded highly. However, the reason that video footage for both tourism and disaster prevention received relatively low scores could be related to the fact that the users did not have enough time to watch the videos thoroughly.

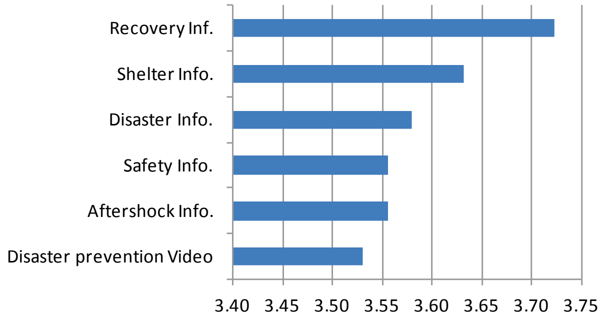


Figure 14. Usefulness of disaster prevention information obtained via 1Seg

4) Comprehensive evaluation of information transmitted

As shown in Fig. 15, on the whole, transmission via 1Seg received a higher evaluation than that via the Internet. In particular, for the question “Did you find the information you wanted?” the level of satisfaction was higher for information obtained via 1Seg. It appears that 1Seg is better at sorting and presenting information considered to be important, and that there are comparatively few people who want in-depth information unique to certain regions such as that provided by SNSs.

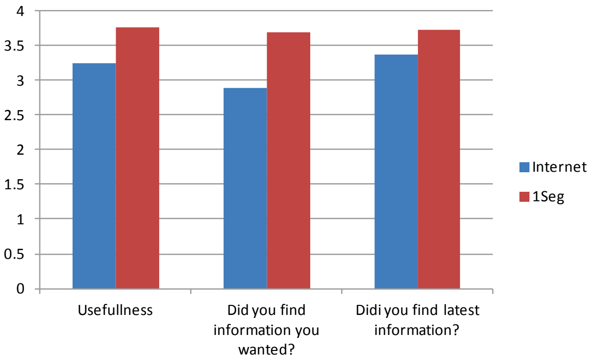


Figure 15. Comprehensive evaluation of information transmissions

5) *Profile of subjects*

Profiles of the participants showed a ratio of around 60% men and 40% women, of which almost half were in the age group 60 to 70 years old. Moreover, visitors from Nagano prefecture comprised 30% of the participants, those from Tokyo 23%, and those from Aichi prefecture 17%, with the remainder from other regions. The percentage of first time visitors was 23%, with the rest having visited the area two or more times.

Listed below are comments by the test subjects entered in the open section of the questionnaire.

- I see that this type of service is available, but if you made it so that advertisements, announcements and general information could be quickly understood by visitors, the service would be better. (male, 40 years old)
- I think it is a big help that climbers and such can view weather information in real time. (female, 20 years old)
- When viewing on a smartphone and such with a small screen, if there is a lot of information, isn't it difficult to read? (male, 40 years old)
- The elderly find it difficult to operate devices, and even though such new information is available, it's often the case we cannot obtain it easily. (female, 60 years old)
- I am very interested in this. I think it's great. (male, 20 years old and male, 40 years old)
- The 1Seg content is much easier to understand and I think it's good. (female, 30 years old)

VI. Summary and What Lies Ahead

The Japanese Tourism Agency is promoting the Regional Tourism Development Platform for tourism, while the Ministry of Internal Affairs and Communications is improving awareness of the necessity for a regional information platform by promoting the public information commons for disaster prevention.

As the main objective of this research, we constructed an experimental website for a communication broadcasting cooperative transmission system and developed a regional information platform. We also performed a small-scale demonstration experiment at Chino station.

Results of the questionnaire show that there was high demand for information focusing on the region, as was initially expected. Also, for questions on whether information was available that users wanted, the level of satisfaction was higher for information obtained via 1Seg. This implies that 1Seg is better at sorting and presenting information believed to be necessary, and that there are comparatively few people who want in-depth information unique to certain regions such as that presented by SNSs.

Furthermore, there was a high demand for disaster and crime prevention information, and users did not find it unusual that disaster prevention information was provided on the tourist portal.

What can be concluded at this point is that a tourist portal website that uses the regional information platform is useful for users who want to obtain in-depth information unique to a particular region (such as that available on SNSs). However, for users who want to view general information, it appears that 1Seg (data broadcasting) and similar methods, which are able to sort and present information in a format that is easy to find, are better. This raises the question of what ratio of sorted general information to regional in-depth information should be presented on the tourist portal. For example, it seems that the system should dynamically change the ratio of general and in-depth information based on the time, location, and user profile.

Furthermore, we were surprised by the fact that the usefulness of the video information did not score highly. It appears that participants did not want to take the time to watch the video since they were busy and had little time to spare.

For 1Seg, BML data were dynamically changed based on the frequency of the keywords in the regional information database, and a simulation experiment was performed that changed the data broadcast screen. The future plan is to include this type of mechanism into the system, and perform additional experiments using it.

In addition, because the local area government showed interest in the experiment performed during this study, we intend to construct a system with the cooperation of the local government and putting it to practical use.

Acknowledgment

This research was partially supported by the Strategic Information and Communication R&D Promotion Programme (SCOPE) of the Ministry of Internal Affairs and Communications, Japan under Grant No. 122304003.

References

[1] Ministry of Land, Infrastructure, Transportation and Tourism, Japan Tourism Agency, “The Tourism Nation Promotion Basic Plan”, http://www.mlit.go.jp/kankocho/en/kankorikkoku/kihonkeikaku.html (retrieved: November, 2013)

[2] Ministry of Land, Infrastructure ,Transportation and Tourism, Japan Tourism Agency, “Regional tourism development platform”, http://www.mlit.go.jp/kankocho/shisaku/kankochi/platform.html (retrieved: November, 2013)

[3] Chino city, “Chino-City Vision of Tourism promotion,” www.city.chino.lg.jp/www/contents/1365379527687/files/kankouv.pdf (retrieved: November, 2013)

[4] J. Murai, “ICT Architecture for Future Disaster Communication” Journal of Institute of Electronics, Information and Communication Engineers, 95(3), Mar. 2012, pp. 259-264

[5] K. Saitoh, H. Kitayama, and T. Takase, “About the Area Limitation 1Seg Local Service Proof Experiment by Sapporo Snow Festival”、Information Processing Society of Japan, 50(11), Nov. 2009, pp. 1130-1134

[6] A. Nishikawa, “Network-integrated Broadcast Equipment for Local One-segment Services,” Information Processing Society of Japan, 50(11), Nov. 2009, pp. 1135-1139

[7] S. Deguchi, “3-1. Multicast Contents Distribution Service - Present and Future-“ ,The Journal of The Institute of Image Information and Television Engineers Vol. 63 No. 5 , 2009, pp. 590-594

[8] M. Haseyama and T. Hisamitsu, "Common Technologies" of Information Grand Voyage Project Introduction to Image and Video Processing Technologies” The Journal of The Institute of Image Information and Television Engineers Vol. 63 No. 1, 2009, pp. 42-47

[9] The Association for Promotion of Public Local Information and Communication, Japan, “Standard Specification for Local Information Platform” , http://www.applic.or.jp/ (retrieved: November, 2013)

[10] Ministry of Internal Affairs and Communications,“Public Information commons”, http://www.soumu.go.jp/soutsu/shinetsu/sbt/bousai/bousai-kanren-4.htm (retrieved: November, 2013)

[11] T. Miyosawa, H. Hirose, and T.Tsuchiya, ” Regional Information Platform and One-Segment Local Broadcast Service for Tourism Promotion and Disaster Prevention: An initial experiment and assessment,” ICDS 2013, The Seventh International Conference on Digital Society, Feb. 2013, pp. 87-92

[12] T.Miyosawa and W. Kameyama, “Modeling User's Benefit for Hybrid Broadcast and Communication System Optimization” The transactions of the Institute of Electronics, Information and Communication Engineers. B J93-B(4), Apr. 2010, pp. 639-648

Impact of Mobility on Spatial Presence during Audio Narrative Reception

María T. Soto-Sanfiel
Audiovisual Communication and Advertising Departmen
Autonomous of Barcelona University
Bellaterra, Barcelona (Spain)
e-mail: MariaTeresa.Soto@uab.cat

***Abstract*— This exploratory research analyzes the effect of mobile listening on spatial presence during audio fiction consumption. Spatial presence is the feeling of being physically located in a virtual environment or experiencing physical objects as if they were real. A quasi-experimental research was conducted with 2x2 factorial design, the independent variables being listening condition (moving vs. stationary) and two narratives (s1 vs. s2). 327 participants were randomly assigned to each of the experimental situations. For moving listening, they listened to the story while walking around the building and back to the place they started. For stationary, they listened while seated in the same place where the moving condition started. They completed a questionnaire with the spatial presence scale after listening. The main results show that mobility affects attention, spatial situation and high cognitive involvement. Listeners pay less attention to the story, concentrate on it less and it captures fewer of their feelings. Also, the spatial situation (the capacity to imagine the layout, the precise the spatial environment, the calculation of time and the specific mental image of the spaces presented in the story) is lower when the user moves in an open space while listening. Likewise, due to movement, there is less imagination of things related with the story, relation between things in the story itself, activation of thought and perception of the usefulness of the story. These results contribute to the understanding of the psychological processes associated to the reception while on the move.**

Keywords: mobility; reception; audio narratives; spatial presence; psychological processes.

I. INTRODUCTION

This exploratory research observes the effect of mobile listening on *spatial presence* during audio fiction consumption. The general concept of *presence* refers to the feeling of “being there” or “being inside” the scene where the story is unfolding. The phenomenon is often described as the perception of non-mediation [1]. It can be understood as the psychological state in which the person’s subjective experiences are created by some form of media technology, with a scant notion of how the technology shapes this perception [2]. According to Lee, presence is a psychological state in which the experience of virtuality goes unnoticed [3]. Spatial presence is one of the dimensions of presence [4]. It is specifically defined as the feeling of being physically located in a virtual setting or experiencing physical objects as if they were real [5].

There is no known research that explores the effect of the modality of consumption (mobile or stationary) to the reception of sound products, in spite of the proliferation of audio portable devices and audio offers since long ago. The consumption of radio while on the move is nothing new, indeed. Particularly, there is a lack of empirical information on how mobile reception affects the psychological relation between audiences and audio products. In spite of that, there are tentative explanations of the characteristics of mobile listening in urban environments, particularly of music, which have originated from researchers from disparate disciplines. For example, it has been said that the use of earphones fosters the creation of a private listening bubble within a public space The earphones provide the ears with the personally desired listening experience that seeks to eliminate the sounds of congested industrial cities [6]. It has been also stated that the use of earphones produces a spatial experience of individual listening that destroys the perception of external space or position, and reveals the boundaries between private and public listening spaces [7]. As a matter of fact, it has been argued that audiences seek to engage with the media not only to connect, but also to disconnect from the different spheres of reality [8]. Finally, it has been proposed that due to the fact that we experience acoustic saturation because of the constant exchange of sounds caused by different media, modern-day listening is characterized by an overall and disengaged listening in which media sounds form our everyday background [9].

Truax defines listening as a system of holistic interconnection between sound, the listener and the ambience [10]. This suggests that mobile urban listening, produced in physical places that are not designed for projecting sound, or for detailed mediation and exploration by the user, could affect the reception. That idea also implies that the qualities of the social setting in which listening occurs affect the actual sound due to the spatial characteristics of the surrounding urban geography, and the complexity of sounds produced for the spatial and temporal simultaneity of experiences, agents or events occurring within said geography. That idea also suggests that audio content could alter behaviour (e.g. moving in rhythm to music) or the psychological treatment of content or of one’s environment (e.g. reduce attention and/or affect spatial or temporal position).

ISBN: 978-1-61208-324-7

In spite of the lack of known empirical evidence, some other researchers have also speculated about the consequences and/or effects of mobile listening using portable devices. For example, it is believed that the sounds that accompany an everyday action are used as tool for the appropriation of experiences [11]. It is stated that everyday mobile listening embellishes one's own environment, marks frontiers, and controls time and/or learning, too [12]. The general belief is that mobility inevitably changes the way we relate both with sound and space, which, in turn, could affect behaviour [13]. Nevertheless, new listening practices have led to consumer habits that should be observed specifically by content and situation (in terms of mobility) and the listening environment [14][15].

II. METHOD

A. *Participants*

There were 327 university students who cooperated with the research without receiving any compensation. 58.7% were women and 41.3% men. The average age was 21.18 years (Rg = 17-40, *SD* = 3.99). The students were invited to collaborate in the vicinity of the Faculty of Communication Science, at a large University from Spain, where the data was collected.

B. *Procedure*

Quasi-experimental research was conducted with 2x2 factorial design, the independent variables being listening condition (moving vs. stationary) and narrative (s1 vs. s2). The participants were randomly assigned to each of the experimental situations. The narratives used were two horror stories, of high aesthetic quality.

Both listening situations were in the open air. For mobile listening, the participants were asked to listen to the story while walking around the Faculty building and back to the place they started. Having studied the route beforehand, we calculated that this was the distance required to hear the complete story and get back in time to answer the questionnaire immediately after. For stationary listening, the participants were asked to listen while seated in the same place where the moving condition started. All participants, but particularly the moving ones, were asked not to interrupt the narrative and to abstain from communicating with anybody while doing the experiment, as this could spoil the results.

C. *Materials*

The participants answered a questionnaire containing a 35 item *spatial presence* previously formulated scale [16]. It was performed a factorial analysis of it. After different tests, it was agreed that the results offered by the method of varimax rotation and extraction of main components showed the clearest structure. The results revealed the existence of 8 factors that together explain 68.50% of variance. The Kaiser-Meyer-Olkin (KMO) Test value was .881 and Bartlett's Sphericity was 5691.145. The model was statistically significant (*p* <.001) [17].

The results of said procedure were fairly aligned with the proposal of the original scale, with some exceptions. To begin with, a difference was found in the first of the factors, which here contained 8 items. It was found that the factor was the subset of the 4 items that, in the scale's proposal, appeared in the sub-factor self-location of spatial presence, plus the other 4 items of the sub-factor *possible action*, of the same spatial Presence. We therefore decided to call the factor obtained by this study spatial presence. Afterwards, another difference was found in the suspension of disbelief factor in the original scale, which in this study was divided into two different factors. Because of the items forming part of each, they were called persistence of disbelief and suspension of disbelief. Table 1 shows the first four factors that appeared during the validation of the scale and Table 2 shows the next second four.

Eight subscales were formed, each corresponding to one of the factors, based on the sum of the partial scores of each item. We also obtained an overall index of spatial presence from the sum of all scores of all items in the scale. These were incorporated in the analysis.

III. RESULTS

Results show an effect of listening condition on some of the dimensions of the factors. There were found statistical differences for attention (*F* = .769, *t* = -1.93, *p* >.054), which was higher when stationary (*M* = 5.18, *SD* = 1.15, *N* = 168) than when moving (*M* = 4.93, *SD* = 1.15, *N* = 159). Attention to the story, thus, is greater when the receiver is stopped than when he/she is on the go. Listeners pay less attention to the story and concentrate less on it during movement. Moreover, the story captures less their feelings or they full dedication to it. It could be explained by the conjunction of two facts. First, people need to pay attention to their own movements and to the characteristics of the road, for assuring successful displacements. Second, the sounds of the audio narrative could interact with those of the environment. It is expectable that in noisy spaces, like those of densely-populated urban cities, attention to the story could even decrease. The experiment was produced in the calm area that surrounds a within campus school.

There were also found differences for spatial situation (*F* = .665, *t* = -2.58, *p* <.010), which was higher when stationary (*M* = 5.14, *SD* = 1.16, *N* = 168) than when moving (*M* = 4.80, *SD* = 1.21, *N* = 159). Likewise, there was found a tendency towards difference for high cognitive involvement (*F* = .220, *t* = -1.83, *p* >.067), which tended to be greater when stationary (*M* = 4.42, *SD* = 1.15, *N* = 168) than when moving (*M* = 4.18, *SD* = 1.19, *N* = 159). These two results are logical and coherent between them. The first one recognizes that the intellectual characterization of the spatial situation in which the narrative takes place is affected by the movement of the listener.

TABLE 1. FACTORIAL ANALYSIS. ROTATED SATURATION MATRIX OF THE JOINT SAMPLE.
(*N*= 327)
SCALE OF SPATIAL PRESENCE (4 FIRST FACTORS)

	Factors (% variance explained)			
Items	***Self-location and Possible action (28.85)***	***Attention (10.01)***	***Specific terrain of interest (7.33)***	***Spatial situation (6.08)***
I felt like I was in the setting of the story	.601			
It was as if my real position had moved to the setting of the story	.717			
I felt physically present in the setting of the story	.737			
I felt as if I had played a part in the action of the story	.810			
I got the impression that I could be active in the ambience of the story	.819			
I felt as if I could move between the objects in the story	.769			
The objects in the story gave me the feeling that I could do things with them	.762			
I felt I could so what I wanted in the setting of the story	.765			
I paid full attention to the story		.815		
I concentrated on the story		.834		
The story captured my feelings		.693		
I was fully dedicated to the story		.786		
I'm generally interested in the subject of the story			.807	
For some time I felt great affinity with the subject of the story			.808	
I was already a fan of the subject of the story before I heard it			.798	
I love thinking about the subject of the story			.817	
I could imagine the layout of the spaces presented in the story				.671
I had a precise idea of the spatial environment presented in the story				.710
It was impossible for me to calculate the size of the space presented in the story				.806
Even now I have a specific mental image of the space presented in the story				.794

TABLE 2. FACTORIAL ANALYSIS. ROTATED SATURATION MATRIX OF THE JOINT SAMPLE.
(*N*= 327)
SCALE OF SPATIAL PRESENCE (4 SECOND FACTORS)

	Factors (% variance explained)			
Items	***Imag. of visual space (4.85)***	***High cog. Involve. (4.45)***	***Persistence of disbelief (3.74)***	***Suspension of disbelief (3.15)***
When someone shows me a map I can easily imagine the space	.767			
I find it easy to manage a space in my mind without really being there	.800			
When I hear a story I can normally imagine the distribution of the objects described	.746			
When someone describes a space to me, I can normally imagine it easily and clearly	.807			
Most things I was thinking were related with the story		.600		
I only thought a tiny bit about the things in the story being related with others		.699		
The story made me think		.658		
I wondered whether the story would be useful for me		.519		
I concentrated on working out whether there were any inconsistencies in the story			.782	
I took a critical stance with respect to the representation of the story			.782	
I paid no attention to the existence of errors or inconsistencies in the story				.751
It didn't matter to me if the story contained errors or contradictions				.809

Considering all of the above, it means that the capacity of imagining the layout of the spaces presented in the story, the precision of the idea about the configuration of the spatial environment recreated by the narrative, the calculation of the size of the space in which the story develops, and the specific mental image of the space recreated are greater when the listener is stopped than when is moving. Besides, results show that the intellectual link with the narrative decreases on the move. In comparison when they are stationary, listeners who move think less about things related to the story, about the relation of the story with other people, about the personal usefulness of the narrative, and about the thoughts provoked by the story. All of this confirms that the intellectual involvement with the audio narrative, probably because of the effect of the lowering of attention, is affected by the mode of consumption.

Regarding the effect of the story on the factors that define spatial presence, we found statistical differences for cognitive involvement (*F* = 2.159, *t* = -2.13, *p* =.034), which was higher for s2 (*M* = 4.44, *SD* = 1.22, *N* = 162) than s1 (*M* = 4.16, *DS* = 1.11, *N* = 165). We also found differences for persistence of disbelief (*F* = .305, *t* = -2.03, *p* >.043), which was higher for s2 (*M* = 4.44, *DS* = 1.50, *N* = 162) than for s1 (*M* = 4.10, *SD* = 1.50, *N* = 165). Finally, we found a tendency towards difference for special interest (*F* = 1.67, *t* = -2.07, *p* >.039), which tended to be greater for s2 (*M* = 3.92, *SD* = 1.52, *N* = 162) than for s1 (*M* = 3.56, *SD* = 1.64, *N* = 165).

IV. Conclusions

The reported results led us to conclude that mobility during audio narrative reception affects attention, spatial situation, and high cognitive involvement. Particularly, mobility causes attention to the audio product to be lower: listeners pay less attention to the story, concentrate on it less and the narrative captures fewer of receivers' feelings.

Also, when the user moves in an open space while listening, spatial situation (the capacity to imagine the layout, the precise the spatial environment, the calculation of time and the specific mental image of the spaces presented in the story) is lower.

Likewise, due to movement, compared to stationary listening, there is less imagination of things related with the story, relation between things in the story itself, activation of thought and perception of the usefulness of the story.

This result makes sense given the experimental conditions of our study: the participants listened in the open air with no restrictions on movement in space (although those in the stationary condition were asked to remain seated). But it suggests something else, in light of the contributions regarding acoustic aesthetics [19]: during non captive audio consumption, and in which movement is possible, in the definition of the psychological state of spatial presence there could be interaction between the localization and perception of actions possible in the real world, and those of the story's imaginary world. The sensation of being situated in the mediated space [20], and in the real physical space in which the mediation occurs, may interact. So, although presence is a psychological state in which the qualities of the media are more influent than the inherent properties of the experience [21], this would also have an effect.

All this data, of which we know of no previous equivalents, contribute to the study of the formation of mental images, especially those produced by audio or radiophonic products [18] and their relation with behaviour. In this sense, further studies could observe the effect of audio narrative engagement in movement itself and in the relation of listener to specific behaviours. In fact, it is somehow surprising that, in spite of the long history of radio contents, their consumption while moving through different means, and the proliferation of portable audio devices, this topic had not been investigated previously. In the light of the creative possibilities that new digital technologies offer to the production of all kind of contents, the results of this study could be useful for conceiving more effective contents, messages, products, and modes of consumption. Apart from being of the interest of digital contents producers and technological developers, the results of this study could be useful for audiovisual regulatory authorities. These studies can also be of interest to different scientific disciplines (e.g., psychology, neuropsychology, acoustics, aesthetics, audiovisual communication, engineering, or narrative studies). Given that this investigation only examined the effect of behaviour on psychological responses to narratives, a first reverse study could be made of the effect of psychological responses on specific aspects of behaviour.

Acknowledgment

This study is part of a bigger research that explored the effect of the consumption mode on narrative engagement. The complete results of the project are expected to be published during 2014 [22].

The author expresses her gratitude to Erika Arámbula, Ignacio Bergillos, and Luis Felipe Ugalde for their cooperation in the data collection.

References

[1] M. Lombard and T. Ditton, "At the heart of it all: the concept of presence", Journal of Computer-Mediated Communication, vol. 3, 1997, pp.1–39.

[2] R. Tamborini and P. Skalski, "The role of presence in the experience of electronic games" in P. Vorderer, and J. Bryant, Eds. Playing Videogames. Motives, Responses, and Consequences, Lawrence Erlbaum, Mahwah, NJ, 2006, pp.225–240.

[3] K.M. Lee, "Presence: explicated", Communication Theory, vol. 14, 2004, pp.27–50.

[4] R. Tamborini and P. Skalski, "The role of presence in the experience of electronic games" in P. Vorderer, and J. Bryant, Eds. Playing Videogames. Motives, Responses, and

Consequences, Lawrence Erlbaum, Mahwah, NJ, 2006, pp. 225–240.

[5] K.M. Lee, “Presence: explicated", Communication Theory, vol. 14, 2004, pp. 27–50.

[6] M. Bull, Sounding out the City: Personal Stereos and the Management of Everyday Life. Oxford: Berg, 2000.

[7] B. Blesser and L-R. Salter, Spaces Speak. Are You Listening? Experiencing Aural Architecture, Cambridge: MIT Press, 2007.

[8] N. Couldry, S. Livingstone, and T. Markham, “Connection or disconnection?: tracking the mediated public sphere in everyday life”, in R. Butsch, Ed., Media and Public Spheres, New York, NY: Palgrave Macmillan, 2007, pp.28–42.

[9] M. Droumeva, “Understanding immersive audio: a historical and socio-cultural exploration of auditory displays”, Paper presented at ICAD 05-Eleventh Meeting of the International Conference on Auditory Display, Limerick, Ireland, 6–9 July, 2005, pp. 162-168 [retrieved: January, 2014, from http://www.icad.org/Proceedings/2005/Droumeva2005.pdf]

[10] B. Truax, Acoustic Communication, 2nd ed., Westport, CT.; Ablex Pub., 2000.

[11] P. Rebelo, M. Green, and F. Hollerweger (2008) “A typology for listening in place”, Proceedings of the 5th International Mobile Music Workshop, 13–15 May, 2008, University of Applied Arts, Vienna, pp.15–18 [retrieved: January, 2014, from http://mmw2008.dieangewandte.at/MMW_PDF/MMW_proceedings2008_web.pdf#page=15].

[12] A. Williams, Portable Music and Its Functions, New York, NY: Peter Lang Publishing, 2006.

[13] P. Rebelo, M. Green, and F. Hollerweger (2008) “A typology for listening in place”, Proceedings of the 5th International Mobile Music Workshop, 13–15 May, 2008, University of Applied Arts, Vienna, pp.15–18 [retrieved: January, 2014, from http://mmw2008.dieangewandte.at/MMW_PDF/MMW_proceedings2008_web.pdf#page=15].

[14] P P. Rebelo, M. Green, and F. Hollerweger (2008) “A typology for listening in place”, Proceedings of the 5th International Mobile Music Workshop, 13–15 May, 2008, University of Applied Arts, Vienna, pp.15–18 [retrieved: January, 2014, from http://mmw2008.dieangewandte.at/MMW_PDF/MMW_proceedings2008_web.pdf#page=15].

[15] M. van Zeijl, M. (2011) The Sound Walker in the Street. Location-Based Audio Walks and the Poectic Re-Imagination of Hybrid Space, MA-Thesis, University of Utrecht, 23 May, 2011, pp. 1-81 [retrieved: Januart, 2014, from http://igitur-archive.library.uu.nl/student-theses/2011-0909-200759/3207803_TheSoundwalkerInTheStreet.pdf]

[16] P. Vorderer et al., MEC Spatial Presence Questionnaire (MECSPQ): Short Documentation and Instructions for Application, Report to the European Community, Project Presence: MEC (IST-2001-37661), 2004, pp. 1-14 [retrieved: January, 2014, from http://www.ijk.hmthannover.de/presence].

[17] G. W. Snedecor and W.G. Cochran, Statistical Methods, 8th ed., Ames; Iowa State University Press, 1980.

[18] E. Rodero, “See it on a radio story. Sound effects and shots to evoked imagery and attention on audio fiction”, Communication Research, vol. 39, No. 4,2012, pp.458–479.

[19] B. Truax, Acoustic Communication, 2nd ed., Westport, CT.; Ablex Pub., 2000.

[20] M. Lombard and T. Ditton, “At the heart of it all: the concept of presence”, Journal of Computer-Mediated Communication, vol. 3, 1997, pp.1–39.

[21] A. Sacau, J. Laarni, and T. Hartmann,”Influence of individual factors on presence”, Computers in Human Behavior, vol. 24, 2008, pp.2255–2273.

[22] M.T. Soto-Sanfiel, “Engagement and mobile listening”, International Journal of Mobile Communication, in press.

Building Trust in the Cloud Environment: Towards a Consumer Cloud Trust Label

Lisa van der Werff, Theo Lynn, HuanHuan Xiaong, Graham Hunt, John Morrison, Philip Healy, David Corcoran

Irish Centre for Cloud Computing and Commerce
Dublin City University
Dublin 9, Ireland
e-mails: {lisa.vanderwerff@dcu.ie, theo.lynn@dcu.ie, huanhuan.xiong@dcu.ie, graham.hunt@.dcu.ie, j.morrison@cs.ucc.ie, p.healy@cs.ucc.ie, david.corcoran22@mail.dcu.ie}

Abstract— **Low consumer trust presents a significant barrier to cloud service adoption and the growth of the cloud industry. The cloud environment is generally perceived to have high levels of uncertainty and risk. Trust plays a central role in allowing consumers to overcome this risk when making adoption decisions. This paper discusses the characteristics of cloud services that form the basis for consumer trust decisions and argues that service providers need a more transparent, accessible method of communicating these characteristics to potential consumers. As such, this paper is directly relevant to conference tracks discussing consumer-oriented digital services and in particular the topic of consumer trust in digital society. Drawing on the nutrition label concept and aspects of previous computational trust models, we propose a dynamic trust label for cloud computing. The cloud trust label aims at present real time and cumulative metrics to consumers in an easily understandable format. In doing so, the label can be used to aid knowledge based trust decisions and ultimately encourage adoption of cloud services.**

Keywords-cloud computing; trust; nutrition label; risk.

I. INTRODUCTION

Cloud computing can be described as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (National Institute of Standards and Technology, NIST [1]). The information technology (IT) related savings for cloud computing include lower implementation and maintenance costs; cost of power, cooling, storage and paying only for what is used [2]. There are also operational benefits due to the flexibility and agility of cloud computing. According to the European Commission, cloud computing has the potential to generate €250 billion in gross domestic product (GDP) with the creation of 2.5 million jobs by 2020 [3].

A number of factors are cited as barriers to wider cloud adoption by consumers. These include issues with trust, security and transparency [4], which introduce high levels of risk and uncertainty and prevent more widespread cloud adoption. Improving our understanding of the factors underlying consumer trust decisions is vital to capitalising on the potential benefits of cloud computing.

Previous research aimed at improving trust in the Cloud has focused predominantly on technical aspects of data handling and assigning accountability for potential issues to specific parties in the chain of service provision [5]. This focus emphasises methods of preventing and handling trust violations but fails to explain the role of consumer expectations and perceptions in driving their initial trust and adoption decisions. This paper takes a consumer-oriented view of trust in cloud computing and examines the risks inherent in the cloud environment and the characteristics of cloud technology which consumers are likely to assess in making trust judgements. Building on work done on nutrition labels and computational trust models, we propose the use of a trust label for cloud computing that will allow Cloud Service Providers (CSPs) to signal dynamic trustworthiness information to consumers.

The remainder of this paper is organised into three sections. First, we will discuss issues of risk and uncertainty in the cloud environment including the selection of CSPs, the characteristics of cloud computing and the legal issues which impact consumer cloud experiences. Second, we will explore the theoretical underpinning of consumer trust perceptions and provide a brief overview of relevant literature on trust in the field of information systems. Finally, we examine previous research into the use of nutrition labels to communicate information in the context of information systems and outline our plans to develop a label specific to developing trust within the Cloud industry.

II. RISK AND UNCERTAINTY IN THE CLOUD ENVIRONMENT

Cloud computing provides compelling benefits and cost saving options for consumers [4]. However, adopting cloud computing services presents new risks and uncertainty that increases the perceived complexity of the adoption decision-making process and cloud provider selection [2]. The Cloud can introduce a single point of failure as demonstrated by Amazon EC2 outage in 2011 [6] and raises concerns over the security of data as demonstrated by the recent controversy over NSA surveillance [7]. CSPs need to look for mechanisms that can address such risk factors.

In adopting cloud services, the user is making a commitment to a CSP and needs to understand the possible impact of selecting the wrong CSP, security and data privacy risks that are inherent in the cloud environment, as well as the legal issues that are currently leading to uncertainty.

A. Cloud Service Provider Selection

For enterprise consumers, the economic appeal of adopting cloud computing is often depicted as “converting capital expenses to operating expenses” [8]. The perceived benefit is that by removing the up-front capital expense the user transfers the risk of overprovisioning or underprovisioning and frees up capital for core business activities [8]. However, accurately comparing CSP’s pricing schemes can be challenging with providers using different pricing models making the selection process difficult [9]. Although cloud computing is cost effective and cost transparent, incorrect CSP selection will lead to a user paying more than expected [9]. Consumers can easily become locked-in and dependent on a vendor such that they cannot terminate the relationship without incurring substantial financial costs [10]. This is a significant concern for consumers as it reduces their flexibility to move between CSPs and reduces the consumer’s bargaining power [11]. CSPs will often design lock-in into their services through the use of closed architectures to reduce portability and ease of data migration [11]. As a result, selecting a CSP is most likely the beginning of a long-term relationship that will be difficult to break.

B. Cloud Computing Characteristics

The five essential characteristics of cloud computing as set out by NIST [11]: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service suggest flexibility and ease of use for the consumer. However, these characteristics convey a contradictory message in the context of technology decision-making by introducing new risks and uncertainty [5]. For example, in outsourcing to a CSP the consumer faces similar concerns to those involved in a traditional outsourcing decision whereby they are limiting their control over the service while still retaining responsibility for it [5]. They are paying for a measured service yet have no control over its measurement. Hosting application and data in a multi-tenant environment increases consumer uncertainty related to privacy, compliance, integrity and confidentiality among other concerns [2].

C. Legal Issues

As a result of lack of consumer control over cloud resources, they must rely on contracts or other formalised trust mechanisms to try encourage appropriate usage [5]. It has been suggested that the contract between the consumer and CSP can often lead to further uncertainty [11]. One of the difficulties is that existing legislation was not written with the Cloud in mind [11]. A number of common legal issues are outlined below.

- **Security and Data Protection** are continually ranked among the top barriers to cloud adoption [2][4]. For many consumers, the perceived risk is still too high to place critical personal information in the Cloud. Possible risks include increased vulnerability of data being accessed by third parties through surveillance by national security agencies, malicious users, data leakages, failure of electronic and physical transport systems for data and back up (if carried out) [2]. In many cases, legal agreements for cloud services seek to place the responsibility for security and data protection on the data owner, i.e., the consumer, to ensure a level of security appropriate to the risks represented by the processing of the data [11][12]. Another factor causing uncertainty is many standard terms of CSPs do not necessarily require security incidents to be reported to the consumer [13]. Consumers must also consider the security and location of their data while in transit. Many cloud legal agreements specify that data will be stored and processed within certain regions but do not specify that they will not be transferred outside these limits [11].

- **Service Levels and Performance** – The Service Level Agreement (SLA) will typically contain a defined list of services delivered, performance targets, auditing mechanisms and any compensatory mechanisms [11]. However, uncertainty is introduced as many SLAs rely on the chain of service provision; this may mitigate any commitment by the CSP to performance [11]. Many CSPs, typically, reserve the right to amend contract terms unilaterally where continued use is deemed acceptance resulting in continued uncertainty for the consumer [14]. Often consumers cannot monitor performance levels and are reliant on information provided by the CSP [11].

- **Data integrity** refers to maintaining and assuring the accuracy and consistency of data over its life cycle [15]. Many consumers consider the Cloud as a safe method of backing up their data. As a result, data integrity is core to consumer expectations [11]. A recent study found that the majority of CSPs place the legal responsibility for preserving the data integrity with the client increasing their potential risk [14].

- **Choice of jurisdiction** – The nature of cloud computing assumes that data will be stored across multiple data centres by a CSP introducing a degree of jurisdictional uncertainty even if stated in the contract [11]. With almost 50 per cent of CSPs choosing US jurisdiction, there is a disincentive for consumers to take legal action due to the high costs of dispute resolution [11]. In many cases, CSPs that choose a US state as applicable law seek to deny any liability for damage as far as possible and restrict compensation to service credit [14]. This can result in significant financial losses for the consumer. However, it should be noted that EU law, typically, does not allow providers to contractually avoid liability to the extent of the US legal system.

- **Termination** – A commonly cited issue for consumers is the ability to retrieve and transfer their data on leaving the CSP [11]. Most providers fail to provide assistance in off boarding data and those that do tend to charge for it. This increases the chances of a consumer becoming locked-in to the CSP. Furthermore, the standard terms of the contract often provide little grace period for consumers to migrate their data [11].

To increase cloud adoption, the above risks and uncertainty need to be addressed.

III. Signalling Trust in the Cloud

In contexts where individuals perceive high levels of risk and uncertainty, trust provides a vital basis for interdependence and cooperation between two parties in a relationship [16]. Indeed the existence of risk is a necessary condition of trust in another party. Improving consumer trust in cloud services provides an important opportunity for consumers themselves, and for the cloud industry as a whole, in overcoming high levels of risk and uncertainty and paving the way for cloud adoption.

Trust is considered a three stage process consisting of the forming of positive expectation, the decision to make oneself vulnerable to another party and a risk taking act [17]. This sequencing of events has important implications for the approach that cloud service providers might take to increasing consumer trust and reducing perceptions of risk and uncertainty in the cloud environment. In order to encourage cloud adoption, which might be seen as a risk taking behaviour, providers must focus on how to increase positive expectations (stage 1) and drive consumer willingness to be vulnerable (stage 2) despite the risks perceived in their environment.

A considerable body of literature in the field of interpersonal and organisational trust has been devoted to uncovering the factors which contribute to positive trust expectations. The dominant model in the trust literature was put forward by Mayer et al. [18] and proposes that expectations consist of trustworthiness perceptions formed on the basis of the perception of characteristics of the other party. Specifically, three key characteristics are assessed: ability – the competence, knowledge and skills of the other party; benevolence – the extent to which the other party is expected to act in the trustor's interests; and, integrity – the other party's adherence to a set of acceptable principles and rules.

Although this model was originally designed to capture the interpersonal trust process, it has proven to be robust across levels of analysis [19] and is frequently applied to improving our understanding of trust in organisations across a range of industries. A small body of literature has recently developed and adapted the trustworthiness model to the context of trust in technology [20][21]. The primary difference in this context is that the party in which trust is placed is incapable of consciousness or moral agency which prevents it for example from making a decision about whether or not to behave in a benevolent manner [22]. However, trust is a psychological state [23] that exists in the mind of the trustor. Accordingly, theorists [22] suggest that interpersonal theories of trust are useful in understanding trust relationships between humans and technology as long as the human party is making the trust assessments and decisions. In other words, it is logical to apply existing trust theory to understand humans trusting technology but not vice versa.

The traditional trustworthiness model of ability, benevolence and integrity has been adapted in the information systems literature to provide a more suitable assessment of the trustworthiness characteristics of an IT artefact [20][22]. It is suggested that assessments of trustworthiness in this context are built on consumer perceptions of performance, helpfulness and predictability [22]. Performance relates easily to the original dimension of ability in that it refers to the consumer's perception of the competence of the product and its ability to help them to carry out the required task. Helpfulness is proposed as a substitute for benevolence and describes the consumer's perception that support in the use of the product is available. Finally, predictability, related to the original dimension of integrity, refers to the consumer's perception that they can both understand and predict the behaviour of the technological product. Together knowledge and perception of these three characteristics provide a basis for consumer trust in technology.

Trust built on knowledge of the characteristics of a cloud service has an important advantage over trust built on a simple calculation of the risks and benefits of cloud product adoption. Knowledge based trust is likely to be less suspicious and fragile than that based on pure calculation of potential costs and benefits [24][25]. Building robust trust relationships with consumers is advantageous for cloud service providers as it allows a greater threshold for the acceptance of small violations of consumer expectations. Knowledge based trust is also advantageous for cloud consumer as once the trust relationship is established less time is needed for the vigilant monitoring of the service allowing users to fully realise the benefits of the service. However, the online environment is a context in which an overwhelming array of information is available to consumer. Although consumers are motivated to evaluate the trustworthiness of information they access online, the thoroughness of this evaluation is limited by time and cognitive resource constraints. In order to realise the benefits associated with trust, the challenge for the cloud industry lies in devising an effective means of communicating trustworthy characteristics to the consumer. For a thorough review of trust in online environments see Grabner-Krauter and Kalushcha [26] and Beldad et al. [27].

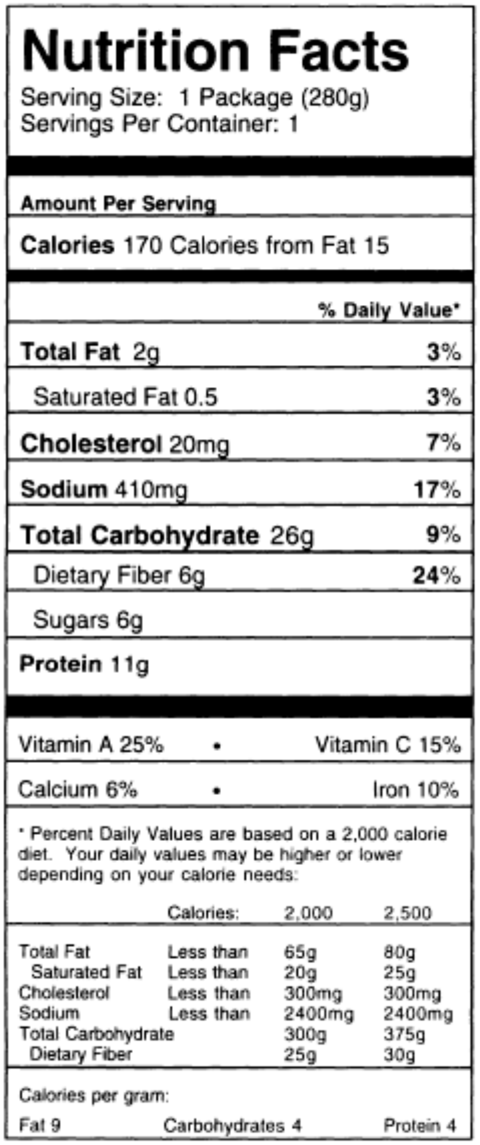
Computational trust models have existed in the field of information systems for many years, typically known as reputation mechanisms [28]. Information related to past behaviours of users is used to determine the reputation of those users in terms of availability, reliability, good quality and security. The mechanism is generally implemented based on a centralized rating model so that the customers and sellers can rate each other using numerical scale or feedback comments (e.g., Amazon, eBay, Taobao, etc.).

Within the cloud computing literature, researchers are beginning to recognize the need for a mechanism to build consumer trust in the Cloud. The traditional reputation mechanism has been extended to distributed systems to meet the challenges of cloud computing [29]. Vu et al. proposed peer-to-peer (P2P) web service discovery that uses Quality of Service (QoS) data and user feedback to rank and select services [30]. The use of SLAs and business activities monitoring is suggested as a method to guarantee the quality of cloud services [31]. In a similar vein, Bogataj and Pucihar suggest a trust building mechanism for cloud computing adoption, which consists of authentication, system security, service quality and non-repudiation [32]. Lynn et al. [33] recently outlined the use of a trustmark to help consumers of cloud computing to build trustworthiness. Trustmarks typically involve one or more of six elements: a declaration of best practice, a subscription to a code of conduct, scrutiny for membership, sanctions for failure, recourse for wrongful revocation, and a remedy for aggrieved customers [33]. They are proposed to build trust by providing evidence of third party certification and have been demonstrated as an effective mechanism for increasing credibility and consumer trust online [34].

IV. A NUTRITION TRUST LABEL FOR CLOUD COMPUTING

In the United States, a Nutrition Labelling and Education Act (NLEA) [35] was signed into law in 1990 that gives the Food and Drug Administration (FDA) [36] authority to require nutrition labelling of the majority of food products. The purpose of the food nutrition label is to play a role in informing consumers about their food purchasing decisions by supporting and supplementing other nutrition education strategies [37]. For instance, offering nutrient content claims and certain health messages, providing quantitative information about nutrients and making it easy to compare between a small set of items. The provision of Nutrition information on food packaging allows consumers to make more informed decisions about their nutrition and adapting their purchase behaviour to suit their individual dietary needs [38]. The typical nutrition label is shown in Figure 1.

The nutrition labelling mechanism has gained wide recognition around the world, and built a broader understanding of practices used in designing and defining labelling requirements [39].



Nutrition Facts

Serving Size: 1 Package (280g)
Servings Per Container: 1

Amount Per Serving

Calories 170 Calories from Fat 15

	% Daily Value*
Total Fat 2g	**3%**
Saturated Fat 0.5	**3%**
Cholesterol 20mg	**7%**
Sodium 410mg	**17%**
Total Carbohydrate 26g	**9%**
Dietary Fiber 6g	**24%**
Sugars 6g	
Protein 11g	

Vitamin A 25% • Vitamin C 15%

Calcium 6% • Iron 10%

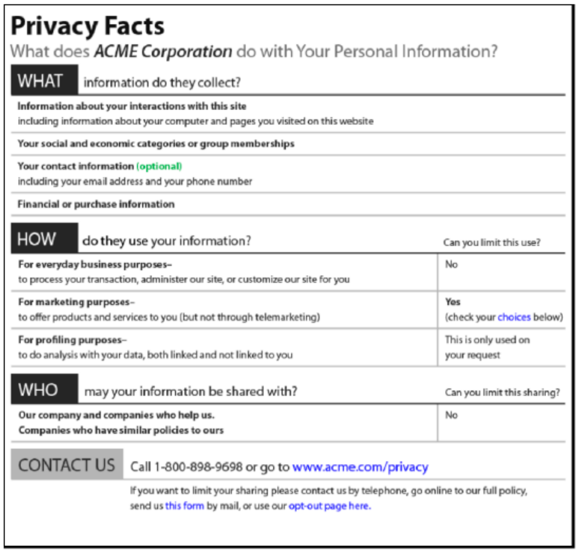
* Percent Daily Values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs:

		Calories:	2,000	2,500
Total Fat	Less than		65g	80g
Saturated Fat	Less than		20g	25g
Cholesterol	Less than		300mg	300mg
Sodium	Less than		2400mg	2400mg
Total Carbohydrate			300g	375g
Dietary Fiber			25g	30g

Calories per gram:
Fat 9 Carbohydrates 4 Protein 4

Figure 1. the Food and Drug Administration's Nutrition Fact panel as regulated by the NLEA, [41]

Carnegie Mellon has demonstrated the transferability of the nutrition label concept to the technology industry in their recent development of a privacy nutrition label [39]. Their work builds on the Platform for Privacy Preferences (P3P) expandable Grid that presents a "nutrition facts" pattern where consumers can investigate and explore the privacy policy of websites [40]. P3P was created by the World Wide Web consortium for encoding and sharing online privacy policies in a standard format (i.e., XML Schema Definition Standard), which can be retrieved automatically and interpreted easily by consumers [42]. Drawing on this, a privacy nutrition label was proposed aiming to simplify the P3P Expandable Grid to enhance user experience by reducing clutter and simplifying symbols [39]. An early stage, simplified label is shown in Figure 2.



Privacy Facts

What does ***ACME Corporation*** do with Your Personal Information?

WHAT information do they collect?

Information about your interactions with this site
including information about your computer and pages you visited on this website

Your social and economic categories or group memberships

Your contact information (optional)
including your email address and your phone number

Financial or purchase information

HOW do they use your information?	Can you limit this use?
For everyday business purposes– to process your transaction, administer our site, or customize our site for you	No
For marketing purposes– to offer products and services to you (but not through telemarketing)	**Yes** (check your choices below)
For profiling purposes– to do analysis with your data, both linked and not linked to you	This is only used on your request

WHO may your information be shared with?	Can you limit this sharing?
Our company and companies who help us. **Companies who have similar policies to ours**	No

CONTACT US Call 1-800-898-9698 or go to www.acme.com/privacy

If you want to limit your sharing please contact us by telephone, go online to our full policy, send us this form by mail, or use our opt-out page here.

Figure 2. the simplified Privacy Nutrition Label, [39]

CMU's proposed Privacy Nutrition Label represents three main concerns:

- **What** kind of information is collected, such as IP address, email address, name.
- **Who** will share or use this information, such as current company or third party.
- **How** this information is used, such as regular navigation, tracking, personalization or telemarketing.
- **Contact Information** to allow the user to obtain further information and support.

CMU's privacy nutrition label provides a good example of how the nutrition label concept increases clarity and availability of information in a technology context. As such, it provides a useful basis for how we might develop a label specific to developing consumer trust in CSPs. However, a number of important questions still remain. It is not yet clear how people will use the label in practice or what quantifiable information provides the best basis for consumer decision-making. In addition, thus far nutrition labels are typically presented as a static representation or logo. In the context of cloud computing, access to real time metrics provides a unique opportunity to present consumers with a continuously updating, dynamic label. Building on this foundation, we propose the use of the nutrition label concept to design a trust label for cloud computing to provide clarity and greater consumer access to information on which to base trust and adoption decisions.

V. THE IC4 CLOUD TRUST LABEL PROJECT

In November 2013, the Irish Centre for Cloud Computing and Commerce (IC4) established a research project to develop and test such a trust label. This project seeks to use a qualitative online Delphi study of cloud industry experts and users to determine the most appropriate format for a cloud trust label, and establish how the risks discussed in Section II can be overcome. The project comprises five rounds of anonymous online interaction between the industry experts and users:

- **Round 1 - Brainstorming:** Discussion to be focused on brainstorming label content.
- **Round 2 – Identifying Label Features:** Finalising a list of label content and discussing the optimal way to communicate this to users.
- **Round 3 – Label Refinement:** Presentation of a draft label design for discussion by the group.
- **Round 4 – Final Label Distribution:** Discussion of label refinement following Round 3.
- **Round 5 – Evaluation:** Evaluation of the final label and process.

Once consensus on label has been agreed, a further research project will be conducted to empirically examine the impact of the label on consumer trust expectations and decisions and to investigate their impact on cloud adoption rates. The theoretical potential of the cloud trust label is clear. However, as consumer perceptions are key, demonstrating the label's practical significance and utility in terms of actual impact on consumer attitudes will be a vital step towards encouraging widespread adoption by CSPs. Separate research on technical systems for monitoring, transferring, analysing and surfacing cloud service data to the trust label securely is required. In particular, attention needs to be given to how the monitoring and analysis performed to calculate the trust metrics can be made minimally intrusive and tamper evident. Finally, consideration will need to be given to the best way of deploying the label and encouraging CSPs to display and communicate this information. Providing convincing evidence of the practical utility of the label for both experts and non-experts will be central to this process. In addition, the label will provide an important benefit to quality service providers by providing an easier means of comparison across services and a clear map of how CSPs might differentiate themselves from their competition.

VI. CONCLUSION

This paper proposed a trust label as a means for cloud service providers to communicate trustworthiness to consumers. In the cloud environment, consumers encounter high levels of risk and uncertainty when making decisions about adopting cloud products. Trust theory suggests that cloud adoption behaviours will be based on consumer knowledge of trustworthiness characteristics that provide a foundation for trust decisions. The effective communication of these characteristics to consumers is vital to improving trust in the cloud environment and maximizing cloud adoption. The dynamic nutrition trust label proposed in this paper provides a means of meeting this communication need. Future research will address the specific content and features of the label and empirically examine its impact on consumer trust and cloud adoption practices.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of Cloud Computing,” National Institute of Standards and Technology, U.S Department of Commerce, 2011

[2] M. Carroll, A. Van der Merwe, and P. Kotze, “Secure cloud computing: Benefits, risks and controls,” Information Security South Africa (ISSA), IEEE, August, 2011, pp. 1-9.

[3] European Commission, “Unleashing the potential of cloud computing in Europe” 2012

[4] D. Bradshaw, G. Folco, G. Cattaneo, and M. Kolding, “Quantitative estimates of the demand for cloud computing in Europe and the likely barriers to up-take” IDC, 2012.

[5] S. Pearson, and A. Benameur, "Privacy, security and trust issues arising from cloud computing." Cloud Computing Technology and Science (CloudCom), IEEE, 2010, pp. 693-702.

[6] J. Pepitone, “Amazon EC2 outage downs Reddit, Quora,”Available: http://money.cnn.com/2011/04/21/technology/amazon_server_outage/, 2011 [retrieved: February, 2014].

[7] G. Greenwald and E. MacAskill, “NSA Prism program taps in to user data of Apple, Google and others,” Available: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, 2013 [retrieved: February, 2014].

[8] A. Fox et al., “Above the clouds: A Berkeley view of cloud computing,” Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, 28, 2009.

[9] U. Onwudebelu and B. Chukuka, “Will adoption of cloud computing put the enterprise at risk?” Adaptive Science & Technology (ICAST), IEEE 4th International Conference, pp. 82-85, October 2012.

[10] K. Zhu and Z. Zhou, “Lock-in strategy in software competition: Open-source software vs. proprietary software,” Information Systems Research, 2011, pp. 1- 10.

[11] T. Leimbach, D. Hallinan, A. Weber, M. Jaglo, L. Hennen, M. Nentwich, S. Strauß, R. Øjvind Nielson, T. Lynn, and G. Hunt. (2013) “Impacts of Cloud Computing. Bericht-Nr. Deliverable No.3 of the STOA Project European Perspectives on impacts and potentials of Cloud Computing and Social Network Sites (Interim Report – Phase III)”, Science and Technology Options Assessment, European Parliament.

[12] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[13] W. Hon, C. Millard, and I. Walden, “Negotiating cloud contracts: Looking at clouds from both sides now,” Stanford Law Review, vol. 16(1), 2012, pp. 79-129.

[14] S. Bradshaw, C. Millard, and I. Walden, “Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services.” In International Journal of Law and Information Technology, vol. 19(3), 2011, pp 187-223.

[15] J. E. Boritz, “IS practitioners' views on core concepts of information integrity,” International Journal of Accounting Information Systems, vol. 6(4), 2005, pp. 260-279.

[16] P. P. Li, "Towards an interdisciplinary conceptualization of trust: A typological approach," Management and Organization Review, vol 3(3), 2007, pp. 421-445.

[17] B. McEvily, V. Perrone, and A. Zaheer, “Special issue: Trust in an organizational context. Organization Science,” vol. 14(1), 2003.

[18] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust." Academy of Management Review, vol. 20(3), 1995, pp. 709-734.

[19] F. D. Schoorman, R. C. Mayer, and J. H. Davis, "An integrative model of organizational trust: Past, present, and future," Academy of Management Review, vol. 32(2), 2007, pp. 344-354.

[20] D. H. McKnight, M. Carter, J. B. Thatcher, and P. F. Clay, “Trust in a specific technology: An investigation of its components and measures,” ACM Transactions on Management Information Systems (TMIS), vol. 2(2), 2011, pp. 12-33.

[21] M. Söllner, A. Hoffmann, H. Hoffmann, and J. M. Leimeister, “Towards a theory of explanation and prediction for the formation of trust in IT artifacts,” In 10th Annual Workshop on HCI Research in MIS, Shanghai, China, December, 2011, pp. 1-6.

[22] M. Söllner, P. Pavlou, and J. M. Leimeister, “Understanding trust in it artifacts – A new conceptual approach,” Academy of Management Proceedings in Florida, USA, August 2013.

[23] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, “Not so different after all: A cross-discipline view of trust,” Academy of Management Review, vol. 23(3), 1998, pp. 393-404.

[24] R. J. Lewicki and B. B. Bunker, “Developing and maintaining trust in work relationships,” Trust in Organizations: Frontiers of Theory and Research, Thousand Oaks, CA: SAGE Publications, Inc., 1996, pp. 114-139.

[25] G. Dietz, “Partnership and the development of trust in British workplaces,” Human Resource Management Journal, vol. 14(1), 2004, pp. 5-24.

[26] S. Grabner-Krauter and E. A. Kaluscha, “Empirical research in on-line trust: a review and critical assessment,” International Journal of Human-Computer Studies, vol 58, 2003, pp. 783-812.

[27] A. Beldad, M. de Jong, and M. Steehouder, “How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust,” Computers in Human Behavior, vol 26, 2010, pp.857-869.

[28] J. Sabater and C. Sierra, “Review on computational trust and reputation models,” Artificial Intelligence Review, vol. 24(1), 2005, pp. 33-60.

[29] P. Resnick and R. Zeckhauser, “Trust among strangers in Internet transactions: Empirical analysis of eBay’s reputation system,” Advances in Applied Microeconomics: A Research Annual, vol. 11, 2002, pp. 127-157.

[30] L. H. Vu, M. Hauswirth, and K. Aberer, “Towards P2P-based semantic web services discovery with QoS support,” Workshop on Business Processes and Services (BPS), in conjunction with the Third International Conference on Business Process Management, Nancy, France, September 2005.

[31] M. Alhamad, T. Dillon, and E. Chang, “SLA-based trust model for cloud computing,” 13th International Conference on Network-Based Information System, pp. 321-324. Takayama, Japan, September 2010.

[32] K. Bogataj and A. Pucihar, “Business model factors influencing cloud computing adoption: Differences in opinion,” 25th Bled eConference Doctoral Consortium, Bled, Slovenia, June 2012.

[33] T. Lynn, P. Healy, R. McClatchey, J. Morrison, C. Pahl, and B. Lee, “The case for cloud service trustmarks and assurance-as-a-service,” 3rd International Conference on Cloud Computing and Services Science Closer'13, Aachen, Germany, May 2013.

[34] K. D. Aiken and D. M. Boush, “Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context specific nature of internet signals,” Journal of Academy of Marketing Science, vol. 34(3), 2006, pp. 308-323.
[35] Nutrition Labeling and Education Act (NLEA) Requirements, Available: http://www.fda.gov/iceci/inspections/inspectionguides/ucm074948.htm, 1994 [retrieved: February, 2014].
[36] FDA, “Labeling & Nutrition”, U.S. Food and Drug Administration, Available: http://www.fda.gov/Food/IngredientsPackagingLabeling/LabelingNutrition/default.htm, 2013 [retrieved: February, 2014].
[37] R. Rothman, R. Housam, H. Weiss, D. Davis, R. Gregory, T. Gebretsadik, A. Shintani, and T. Elasy, “Patient understanding of food labels: the role of literacy and numeracy”. American Journal of Preventive Medicine, vol. 31(5), 2006, pp. 391-398.
[38] A. Gracia, M. Loureiro, and R. M. Nayga Jr., "Do consumers perceive benefits from the implementation of a EU mandatory nutritional labelling program?" Food Policy, vol. 32(2), 2007, pp. 160-174.
[39] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, “A ‘Nutrition Label’ for privacy,” Symposium on Usable Privacy and Security (SOUPS), Mountain View, CA, USA, July 2009.
[40] R.W. Reeder, “Expendable grids: A user interface visualization technique and a policy semantic to support fast, accurate security and privacy policy authoring,” PhD thesis, Carnegie Mellon, Available: http://www.robreeder.com/pubs/ReederThesis.pdf , 2008 [retrieved: February, 2014].
[41] S. B. Keller, M. Landry, J. Olson, A. M. Velliquette, S. Burton, and J. C. Andrews, “The effects of nutrition package claims, nutrition facts panels, and motivation to process nutrition information on consumer product evaluations,” Journal of Public Policy & Marketing, vol. 16(2), 1997, pp. 256-269.
[42] W3C, the Platform for Privacy Preferences 1.1 (P3P1.1) Specification, Available: http://www.w3.org/TR/P3P11/, 2006 [retrieved: February, 2014].

Social Networking Service for Helping Each Other in the Neighborhoods

A User Experience Approach to the Elderly People

Mariana Alejandra Varela
Graduate School of Media and Governance
Keio University
Fujisawa, Kanagawa. Japan
mariana@sfc.keio.ac.jp

Katsuhiko Ogawa
Faculty of Environment and Information Studies
Keio University
Fujisawa, Kanagawa. Japan
ogw@sfc.keio.ac.jp

***Abstract*— This research focuses on the use of Social Network Services among the elderly people in Japan, as a solution that could help to bridge the digital divide in that country. It proposes the creation of a Social Network Service for neighborhoods, in which the relationship among the young and the old is promoted. Existing design and usability guidelines for senior citizens and culture-related issues are highly taken into consideration. User-centered design method is applied to tailor the tool for testing. This paper hopes to bring new insights about how elderly people use Social Network Services in Japan and the usability challenges that they face when trying to use it.**

***Keywords*— Social Network Service; Elderly People; Usability; Japan.**

I. Introduction

The present paper addresses the problem of the aging population as a starting point. This situation affects many countries in the world, but in the case of Japan, is relevant how the population over 65 years old has been increasing year after year. According to the official statistics [1], will become about 30% of the population by 2030.

Although Japan has always been famous worldwide for its great scientific and technologic advances, the statistics show that there is a significant technologic gap between generations. Observing the numbers [2], even though 78% of the population over 60 years old in Japan have a computer, only 23.5% say that use it very often. It is encouraging that over 80% of them believe that the use of Internet is very important. In contrast, in United States of America [3] only 53% of citizens over 65 years old use Internet or email, but 70% of them use it on a daily basis. This remarkable difference shows that having a computer at hand does not necessarily mean its usage.

This papers aims to find a way how the elderly people can integrate better to the Information Communication Technologies. The main Hypothesis is: **It possible through the use of social networks between older adults and younger generations to bridge the technologic gap that separates each other.** It is vital to learn how to design the best user experience, how to successfully improve their everyday lifestyle and how to introduce them in a better way to the digital world. This is a topic that still has not been investigated in full as a possible solution to the digital divide among the senior citizens in Japan.

Some existing services, statistics and researches helped to discover the current state of art. According to the statistics [2], only 7.7%, of the seniors online in Japan use Social Network Services like Facebook, Mixi or Twitter. Among those who use it, they prefer to use Social Networks that include all range of age [4][5] and not those specially made or designed for the seniors (Slownet, Senior Wings, Senior Navi, Senior Com, among others reviewed for this paper). The contrast with the elderly people in America is significant, in which among the active population of senior Internet users, 34% of them use Social Networks like Facebook.

The project “Bring Dich Ein!” in Germany [6], which explores the possibility of the elderly people to post in Internet requests to get favors done around the neighborhood, was a great inspiration to recreate a similar situation in Japan, specially the aspect of geographically limited/closed community and collaboration among them. Parallel to our research with Japanese people, we found many coincidences as the concern for privacy information security and the need of an intuitive design and navigation system. Other similar online services (for example, Ayoudo, Taskrabbit and Kutoto) were also reviewed even they are not specially aimed at senior citizens.

Regarding the use of Internet in general, accessibility barriers that the elderly people go through certainly couldn't be overlooked in this research, specially those related to Independency (to be able to use on their own), Inclusiveness (to be able to use the same technologies as young people) and Terminology (vocabulary easy to understand) [5]. This last barrier, related closely to vocabulary, represented a great concern among the elderly Japanese Internet users.

The paper structure is explained as follows: First, Section II describes the main point that this projects wants to aim. Secondly, the idea generation and selection processes explain the diverse phases that the project went through until now (still ongoing). The background research accounts for not only the bibliographical research but also the field observation and informal interviews. A complete description of the created tool is made, with some examples of scenarios of use is presented in Section IV. Section V

ISBN: 978-1-61208-324-7

reports on how the experience with the users was made. The results and some future work are explained in Section VI.

II. Concept

For setting the boundaries of this research, after researching about online and offline communities, it was decided to make the project in a closed environment: the neighborhood. One can see that the neighborhood is one of the most basic forms of communities, preceded by Family environment and School/Work environment. Working with a small scale was vital to manage this research, given our resources. Also, it was decided that we would aim at only those persons who actually used or wanted to use computers, Internet or technology, as it was not of our interest to find a way to change the attitude of people who are not concerned in overcoming the digital divide.

By talking to the elderly people, some initial assumptions were made: First, one of the reasons why some people are not fond of talking to strangers online is because they have never met face to face in real life and they do not share any bond or reason for interacting. But, if that strange person online is somebody they might have seen around in the neighborhood, they may feel more comfortable and talkative. Elderly people are more likely to stay at home rather than young people, so they may know the faces of the people of the neighborhood.

Second, we found that they feel a little ashamed to ask basic questions related to the technologies, ashamed of not knowing.

By questioning how combining the social environment of the elderly people and their difficulties to for using the technology, we tried to create a nexus where they can meet and eventually settle a solution. For this, we created a two-axis framework: First, an ethnographical study, and second, review and test the design guidelines specifically made to this type of user but applied to this kind of situation and in this country. The design guidelines help as a starting point of what expectations should be considered for designing for the elderly people, and, additionally, we want to discover the cultural and language issues that attain only to the Japanese elderly people.

III. Idea generation

A. Idea generation

The idea generation process was inspired by Bill Buxton's book about User Experiences [7]. It is advised that many ideas should be considered at first; for later choosing the best among them. The complete process of deciding which was the best idea to pursue took around one year, meanwhile bibliographic and field research was made.

There were 7 main ideas generated for the kick-off of this project, always focusing on the elderly people (email service, e-commerce system, social network service, dating site, search engine, online dictionary and online learning site), that were considered, compared, refined and some discharged. Two of them were continued for testing and discussion, and later on, the current project was decided.

We found that without a clear motivation it was going to be hard to test if they could immerse in the Internet and Social Network Services like young people do. We discharged the idea of a service similar to Facebook for the elderly people (they were not interested and current services like that do not show impressive results) and other kind of services like a Dating Site did not include as much users as we hoped to test. On a final term, it was decided to follow the concept of weak bonded generations and the emergence of a tool that works as a node to connect people, rediscover the neighbors and harvest a solidarity spirit among them. (see Section IV for a full description on the idea).

B. Background research

Some papers and publications were taken into account for defining the concept and helped to outline the state of art. However, as a reference to design the User Experience, we considered the usability guidelines for the elderly people that exist up to now. The basis are taken from the *Handbook of Human Factors and Ergonomics Methods* [8], which gives a wide foundation to start working on, and the *Web Content Accessibility Guidelines (WCAG)* created by W3C [9].

Regarding the products and services focused on the senior citizens, Docomo's RakuRaku Smartphone [10] was examined, as much as the books by ”Compyuta Obaachan” (Computer grandma), who explains easily step by step how to operate devices or websites (a special publication about Facebook was reviewed) [11]. A few catalogs and shops were visited, in order to survey which are the physical needs that they suffer, and what they choose in order to make their everyday life easier. Design shape, ergonomics, materials, colors and patterns were analyzed. Needless to say, a wide range of websites and phone/tablet applications were searched online regularly, with special emphasize on those that are a channel for communication among users.

Up to now, three interviews were made and recorded with the Owner and Director of “Mamion”**,** Mrs. Mori, who runs a small school in the center of Tokyo that teaches basic informatics specially to the elderly people. Long and substantial discussions about the senior user were made with Mrs. Mori, who gave us her professional point of view and advice about which are their needs, the concepts that they have difficulties with, and what brings them to learn how to use the computer. She also helped recruiting users for the tests (See section V for a the Testing description)

Above all, and constantly, observation of the elderly people was made in public places like parks, cafeterias, shopping malls, trains and post offices. In addition to taking pictures, also was noted how they communicate, body language, how long they take to make simple and difficult tasks (for example, from operating an elevator control to recharging credit in train card or withdrawing money from an ATM machine).

IV. System Explanation

The concrete tool that is being created, tested and analyzed is an Internet-based Closed Social Network Service for local communities, with a very strong focus on the senior citizens, but where everybody can participate regardless of the age. As a reminder, our main hypothesis is that if old and young people can get together in one virtual space, they can enhance the communication and try to bridge the gap among young and old generations.

The main boundary is that only people from a certain area (neighborhood) can participate, after going through a registration system for verifying the account. Setting this boundary so closed is vital to gain trust among the users and not to fear that outsiders may interfere with their privacy.

Their main motivation expected for participating on the website is helping each other (neighbors helping neighbors) with their needs, doing small favors or just lending a helping hand, where communication and cooperation are the main keywords for making it work, as money is not involved.

The system is called "Manada". It means in Spanish "Large group of animals that move and do things together", Even though the word itself has no meaning in Japanese, it was important to use something easy to pronounce but with a meaning behind that represents the project somehow.

The starting point for conceiving this concept revolves among the idea that young people (younger than 45 years) may already know Social Network Services (Facebook, Twitter among others) and are familiar with this kind of communication technologies, but older people still do not. For some of them, it may be difficult to understand the concept of an online Social Network because the relationships "face to face" are their main way of communication.

This is a very simple scenario of use to illustrate the idea: User A is an old lady who needs some help for a certain task that she can not do because of a physical difficulty. She posts the message asking for help (This posts are called *"Onegai" , which means "a favor" in Japanese*) and waits for a reply. User B is a neighbor who lives very close and sees the *"Onegai"* posted in the Social Network. He replies and helps her. Another example shows that Seniors can also help, and not only receive help: User C is a young housewife who posts an *"Onegai"* on the Social Network Service, and it happens to be something that User D, even though being much older, can do perfectly. He replies and feels good knowing that he can still be useful for someone.

Next, it was important to start making the first tests to evaluate the concept and check if the communication and support across or inter generations is possible through the Social Network Service, creating bonds within the community, and build a theory based on that findings. As many as possible existing design guidelines are being tested and put in practice, in order to verify their validity or not among the Japanese users.

V. Testing experience

According to the user-centered design [12], it is important to include the final user as soon as possible in the design process, in order to analyze their needs and hear their opinion. That is the reason why, after making the first design attempts, it was vital to meet some users, hear their opinion, ideas and test their abilities with our tool.

A. Users

A basic Persona was created to serve as a guide for finding subjects for the test:

1. Be 65 years or older;
2. Be an active user of the computer, without any education restriction, and
3. Japanese native.

B. Testing

The testing was conducted in September and October 2013 in Tokyo and Kanagawa, Japan. Three users were students of the Informatics School "Mamion" and the other two subjects were contacted separately (Fig. 1). Some testings took place at the school and some at the house the users for their comfort.

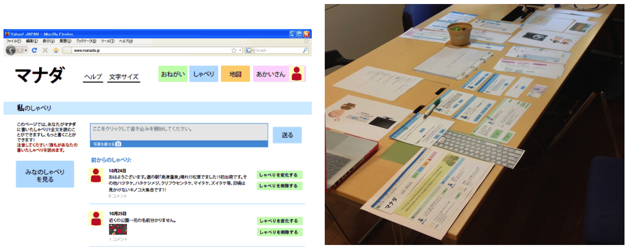
The users at the School were two men (69 and 83 years old) and a woman (73 years old). They were active students of the School and were taking courses because of different reasons: want to keep updated (still feeling young), want to fight boredom, or communicate with family abroad. The other pair of users (Male, 75 years old and Woman 74 years old) did not go to class but learned alone and with the help of their families.

Before starting the test, they were asked to complete a form with some personal information (name and age), and multiple choice questions. On the first question they had to answer what terminal they could use (Personal Computer, smartphone or iPad) because we were concerned to know if this kind of project was worth to be applied for mobile terminals. We also asked about the use of Internet, because we were interested in discovering if they used it for socializing and communicating with others or if they did other activities. The next question was about exactly which Social Network Services they used (if any), mentioning the most famous in Japan (Facebook, Twitter, Mixi, Line). Also, it was vital to know who they talked to through internet, mentioning from the closest friends and family to unknown people. Next part was about the knowledge they had about words and icons: They had to check the words they knew about the Internet vocabulary. Some of them were "Download" or "Home", but also other words that appear in the Japanese version of Facebook, for example "Share" or "Activity log". Also, we asked them to write the meaning of seven icons that are ordinarily used online and offline, for example, "telephone", "mail", "comment", "print", "delete", "edit" and "accept". Lastly, we asked how they came over the difficulties they find in Internet, if they turned to someone (and who) or if they solve it themselves (and how). This questions were key to lay a ground and better interpret their actions during the testing.

They were asked to read a short explanation of what was the test about and how it was going to be conducted. On the last page, it was detailed what they had to do: *"Imagine that you are Mr/Mrs Akai, and you have just bought a new TV. You have no idea how to connect the cables, so you use Manada Social Network Service to ask for help to your neighbors and see if someone has time to help you"*. Three pictures were shown to help them to imagine the situation: A photo of a new TV, a photo of an instruction sheet, and finally an old person scratching his head with a lost look. This set of pictures was on sight all the time, as a reminder of what they had to do.

Many doubts were cleared before staring and, in order to to follow the Think Aloud technique [13], they were encouraged to say aloud about what they were thinking about while doing the test. All the sessions were recorded by camera.

The testing was made using the technique of paper prototypes (Fig. 2) [14]. The prototypes were made using Adobe Illustrator and had the appearance of a high definition wireframe.



このページでは、あなたがマナダに書いたしゃべり1全文を読むことができますし、もっと書くことができます!
注意してください：誰もがあなたの書いたしゃべりを読めます。

ここをクリックして書き込みを開始してください。

10月24日
おはようございます。道の駅「奥津温泉」晴れ!!松茸でました!!初出荷です。その他ハツタケ、ハタケシメジ、クリフウセンタケ、マイタケ、ズイタケ等、日頃は見かけないキノコ大集合です!!
0コメント

10月25日
近くの公園…花の名前分かりません。
1コメント

Figure 2: Paper Prototypes

All the text written was readable text (not dummy test) in Black color 14pt font. Buttons were colored boxes of rounded borders with the text in bold. Each part of the website was represented with a piece of printed paper. The only part that was always visible was the Internet Explorer bar and the Website's head menu. The width of the paper "screen" was of around 25 cm. They touched with a finger the buttons to imitate the mouse click.

Each test lasted around 20-30 minutes with each participant. It was intended to make it short in order not to exhaust the mental concentration of the individuals.

All of them completed the task (to post an *"Onegai"* on Manada) on the expected time satisfactory and were relieved to hear that they did everything correctly, even though it was informed to them that it was fine to fail. The wrapping up was followed by some oral questions regarding what they think about the concept, if they would use the Social Network Service and finally if they felt that it was easy or hard to use.

VI. Conclusion and Future work

1) According to the questionnaire answers, they were not familiar with the use of Social Network Services in general; so, they did not select any. Also, they indicated that they communicate only with friends and family, what proves right our initial assumption that they do not talk to strangers. As expected because their lack of knowledge in Social Networks, words like "Share" and "Update" were also new for them (The Japanese equivalent was used for the testing), as the results with the icons that are related to posting and editing comments. Regarding the difficulties in using the Internet, they seem not very keen on asking for help, they prefer to find the answers alone searching online.

2) When explaining the task, it was very useful to show pictures to help them imagine the situation. Visual aids were important and it was vital to take the time to explain the same thing several times as they forgot or could not understand it at the first attempt. This is something that we will keep on using in the future testing.

3) They mentioned on the closing talk that they felt it was still difficult to understand how the system worked, even though they could read very clearly all the texts. There were some doubts about the button's labels and titles, specifically when they had to manage their *"Onegai"* they did not understand whether the *"Onegai"* was finished or not once they posted. In other words, they could not grasp the dynamics of an Social Network Service completely.

4) The majority of them thought that this kind of service would be very useful and would like to try it "in real life" but they fear that not many elderly people are familiar with the computer, even themselves feel a big insecurity when facing the possibility of having the ability to use it or not.

Regarding the Usability functionalities that are being affected in this research, so far the Learnability factor is the one that is being more compromised. Users not only have to learn how to use the website but also understand a new concept which is how a Social Network Service works. Additionally, because of their age and lack of english education in their school days, they have serious difficulties understanding the Internet Vocabulary, which consists mainly in English words written in Katakana: a sound transcription of foreign words that do not have an equivalent in Japanese language. Also the Memorability factor is affecting due to the use of foreign words, given that they have to learn by heart not only what action is expected after clicking a certain word but also not being able to associate that word to any known synonym in their own language. Keeping in mind the fact memory decline is normal among senior citizens, this represents a double challenge.

The next step in this work in progress is to make a new design iteration to solve the difficulties presented during the test. An extra focus will be made on the labeling, as many common vocabulary was avoided because japanese elderly people may not be familiar with english words. The total elimination of Katakana words is impossible, but better suitable synonyms should be implemented. This was an obstacle expected to arise, so is the difficulty that it presents.

Moreover, it is necessary to keep on working on the interface, in order to put it in a simpler and friendlier way, expecting to make them feel that they have the ability and confidence to use it.

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-324-7

Also, with this test, the paper prototype phase is considered finished to move on to an electronic interface to be tested on the computer. One of the subjects pointed out that if the test was made on the computer it “would not be so easy”; so, we are looking forward to test on a digital device in the next design iteration with at least 15 users, rising the prototype fidelity and adjusting even more the design.

References

[1] Ministry of Internal Affair and Communications. Statistics Bureau, Director-General for Policy Planing & Statistical Research Training Institute of Japan, Statistical Handbook of Japan, 2012, Retrieved on January 21st 2014 from http://www.stat.go.jp/english/data/handbook/c02cont.htm

[2] GF Corporation. Report No.0083000067 Investigation Related to the Use of Internet Among the Elderly, 2013, Retrieved on January 21st 2014 from http://reposen.jp/3530/13/83.html.

[3] K. Zickuhr and M. Madden. Older adults and internet use. Pew Internet & American Life Project, 2012, Retrieved on January 21st 2014 from http://www.pewinternet.org/Reports/2012/Older-adults-and-internet-use/Summary-of-findings.aspx.

[4] L. Gibson, W. Moncur, P. Forbes, J. Arnott, C. Martin and A. Bhachu. Designing Social Networking Sites for Older Adults, Proceedings of the 24th BCS Interaction Specialist Group Conference (BCS ’10). British Computer Society, Swinton, 2010.

[5] S. Sayago and J. Blat. About the relevance of Accessibility Barriers in the Everyday Interactions of Older People with the Web, Proceedings of the 2009 International Cross-Disciplinary Conference on Web Accessibility (W4A) ACM, 2009, pp. 104-113.

[6] P. Koene, F. Köbler, S. Esch, J. Leimeister and H. Krcmar, Design and evaluation of a service-oriented collaborative consumption platform for the elderly, Proceeding of CHI EA '12 CHI '12 Extended Abstracts on Human Factors in Computing Systems, ACM, 2012, pp. 2537-2542

[7] B. Buxton, S. Carpendale, N. Marquardt and S. Greenberg, Sketching Users Experiences – The workbook, 1st ed., Waltham, MA: Morgan Kaufman, 2012, pp.9-12.

[8] G. Salvendy, Handbook of Human Factors and Ergonomics, 4th ed., Hoboken, NJ: Wiley, 2012, pp. 1442 – 1465.

[9] B. Caldwell, M. Cooper, L. Guarino Reid and G. Vanderheiden, Web Content Accessibility Guidelines 2.0 (2008), Retrieved on January 21st 2014 from: http://www.w3.org/TR/WCAG20/.

[10] Fujitsu Corporation. Fujitsu Introduces Raku-Raku Smartphone 2, Tokyo, August 14, 2013. Retrieved on February 3rd 2014 from: http://www.fujitsu.com/global/news/pr/archives/month/2013/20130814-02.html

[11] K. Okawa, Let's learn with Computer Grandma How to Create Own Digital Life History in Facebook, 1st Ed., Tokyo: ASCII, 2012.

[12] J. J. Garret, The Elements of User Experience: User-Centered Design for the Web, 2nd Ed., Peachpit Press, 2002, pp. 19-24.

[13] J. Preece, Y. Rogers, H. Sharp, D. Benyon, S. Holland and T. Carrey, Human-Computer Interaction, 1st ed., England: Pearson Addison Wesley, 1994, pp.621-626.

[14] C. Snyder, Paper Prototyping: The Fast and Easy Way to Design and Refine User Interfaces. 1st ed. San Francisco, CA: Morgan Kaufmann, 2003.

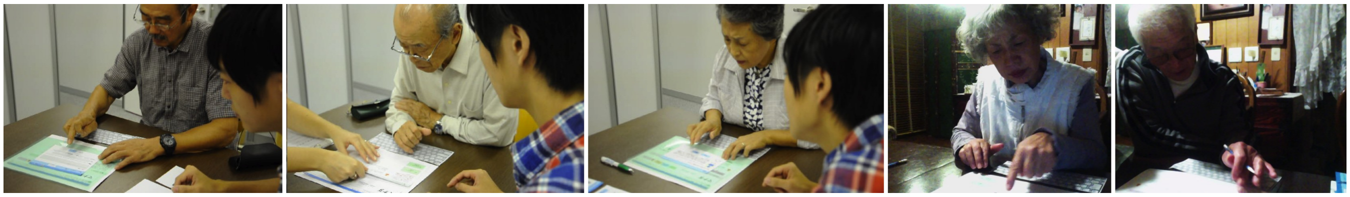


Figure 1. Users taking the test in Tokyo and Kanagawa

Social Networking and Identity Theft in the Digital Society

Eric Holm
Federation University Australia
PhD student, Bond University,
Mount Helen, Australia
e.holm@federation.edu.au

***Abstract* - This paper explores the vulnerability of social network users to identity theft facilitated by the information they share on social networking sites. While social networking presents new possibilities for friendships and the sharing of interests, at the same time it brings vulnerability through the outflow of personal information online. Identity criminals can exploit the weaknesses of social network users and social networking sites, effectively enabling the identity criminal to construct an identity from the information they obtain. The information gathered by an identity criminal can be used to establish identity, a powerful precursor to committing identity fraud. While there are preventative mechanisms that can reduce the incidence of this crime, information sharing on social networks is common and voluntary, which makes it difficult to control. While this paper presents an evaluation of existing work, further empirical research work is needed to understand the vulnerability of personal information on social networking sites. Social networking sites have a vested interest in promoting rather than preventing the sharing of information. In addition, identity crime is pervasive, which makes the amelioration of the risks difficult. In concluding this paper, efforts are made to point toward starting points that will assist in resolving this crime.**

Keywords- social networking; identity theft; identity fraud.

I. INTRODUCTION

Social networking has inspired computer users to share information online. Social networking sites bring together people with common interests and enable mass social interaction to take place. This overcomes geographical constraints and can bring together disparate groups [1]. Social networking is attractive due to its social inclusiveness [2] as well as its interactive nature [3]. For example, 500 million people have used Facebook to create profiles to express themselves across this social networking platform [4]. The social linkages created by such sites bring together new social associations as well as new ways to interact online including instant communication and gaming [4]. In this regard, there have been many narratives about both the positive and negative social implications and influences of this social interaction [5]. Criminal activity has been a negative implication of such interaction and this one seemingly harmless type of human interaction has lent itself to another that is far more sinister: identity crime.

This paper will first consider why the identity crime is serious in the context of the strong uptake of social networking which has been mentioned. The paper will then discuss the responses to dealing with identity crime and social networking that include deliberating the suitability of criminal law and privacy responses to this crime. Thereafter, the paper will discuss the challenges in dealing with identity crime and social networking. Finally, the paper will provide some recommendations arising from this paper and foreshadow future work.

II. THE EMERGING ROLE OF SOCIAL NETWORKING IN INFORMATION SHARING

The extent to which individuals share information on a social networking site is determined by the decisions they make which are influenced by many drivers. The control mechanism used on a social networking site is typically the user privacy settings, which allow an individual to determine the visibility of their social networking profile to others. A social networking profile is the mode in which social networking users represent themselves online and facilitates their existence on the social networking site. The dissemination of information is at the heart of social networking [6]. The opportunity to share information is attractive to users who aspire in particular, to share their emotions, expressions and experiences online [7]. A key driver for social networking sites is the reciprocal nature of such information sharing [8]. Social networking sites finely balance the security needs of user with the ease of use and much of the research around changing the architecture of the interface has been previously explored [9]. Such sharing of information provides the foundation under which many relationships are formed [10] as well as the basis for rekindling relationships with old friends [11]. In addition, many social networking sites also contain incentives for such information sharing to take place whether by promoting the creation of these friendships, sharing general interests or religious beliefs, and numerous other motivators [8]. Many positive outcomes can be derived from social networking.

Social networks have become an alternative to communication in many traditional social contexts [12]. Increasingly communication takes place online and social networking has become a platform that functions in place of (or in conjunction with) existing social contexts. However, social networking is a relatively new phenomenon and many of the social conventions around it are still developing [13]. It may be for this reason that many users are complacent about the potential risks associated with the sharing of personal information on this platform. Studies related to information sharing suggest that gender also influences the preparedness of users to share information, with boys and men being prepared to share information online more freely than girls and women [14]. Furthermore, younger men are seemingly more prepared to share information than older men [15] and it may be that factors like peer pressure play a role in this. Nonetheless, there seems to be complacency in relation to the risks associated with information sharing on social networking sites. Many users share information about themselves that includes their full names, their location, date of birth and also photographs [10]. This can be the information required by identity criminals to form an identity that can be used to perpetrate crime.

When information is acquired by an identity criminal, in most instances it is taken without the knowledge or consent of the victim [16]. In this sense, the victim might not be aware that their information has been stolen until they find themselves exposed to crime-related financial liability. Hence, the motivation for the identity criminal is typically monetary gain [17]. Such crime involves the collection of the information required to replicate the identity of the victim [18]. Once stolen, the identity criminal will typically use the name of the victim to commit fraud: identity fraud [19]. Information taken from a social networking site can be used to establish a false identity. The documents needed to establish identity vary, but most governments accept a range of identification documents to establish it [20]. By world standards, name, gender, nationality and date of birth are considered unique personal identifiers that collectively satisfy identity requirements [21]. Indeed, many of these details are commonly shared on social networking sites. When this information is used, many victims will not know that they have become victims until some considerable time has passed [22]. The time between when an identity crime occurs and an investigation takes place makes it difficult to gather evidence of the crime and to both locate and prosecute the offender [22]. During this time, the victim withstands the frustration of financial losses caused by such crime and research has shown that this frustration worsens the longer it takes for the situation to be resolved [23]. The subversive nature of this this crime ultimately adds to a victim's frustration.

III. WHY IS THIS CRIME SERIOUS?

Identity crime has the potential to reach anyone. Research conducted at Carnegie Melon University suggests that children 15-18 years of age (43%) are the age group most likely to be victimized by identity criminals. Of the other age groups, children aged 11-14 years (28%), 6-10 years (19%) and five years and under make up the balance of victims [24]. However, at the same time, it is evident that children of working age are at risk due to their levels of income as well as their relevant engagement with technology [25]. Overall, these victims present fruitful targets to identity criminals. While it is not clear what the reasons for this might be, it is probable that the risk of victimisation is linked to increased levels of engagement with technology [26]. Inadequate levels of supervision of children's Internet usage, particularly with respect to social networking may also contribute to this [27]. Children have a particular vulnerability to identity theft crime as they usually possess an unblemished personal history and remain relatively undefended as targets of this crime [24]. This increases their status as prime targets of identity criminals. In addition, children often unknowingly share information about themselves that can place them at risk [28]. From these indicators of victimisation, it becomes clear that identity fraudsters are opportunistic when it comes to the perpetration of this crime and anyone can become a victim.

In the United States in 2009, an estimated 11 million Americans had been the victims of identity crime [20]. In 2010, 7% of households in the United States experienced identity theft victimization, [29] amounting to about 8.6 million households [29]. Similarly, in 2010-2011 the estimated cost of personal fraud to Australians was $1.4 billion [30] with approximately 44,700 Australians becoming victims of identity crime [31]. Statistics from the United Kingdom similarly suggest that identity crime is increasing prodigiously with the reported number of cases almost doubling between 2007 and 2012 from 77,500 to 123,600 [32]. These statistics suggest that identity crime is global and significant in terms of both its impact and cost.

The cost of identity crime is often regarded as being comprised of both direct and indirect costs. The most significant cost of identity crime is the financial cost [33]. However, the true cost of identity crime extends beyond financial loss [34]. These have been referred to as the difference between direct and indirect costs or hard and soft costs [34]. The financial costs (the hard costs) are easily quantified whereas the non-financial costs (soft costs) are more difficult to quantify as they relate to the cost of preventative measures as well as damage to reputation [34]. The cumulative losses reflect both the hard and soft costs of identity fraud crime. Obtaining accurate measures of the true cost is also influenced by the lack of data available on this crime [34]. The banking sector suffers significant losses in relation to identity crime [35] but its spokespersons remain reluctant to disclose the losses arising from this crime. Interestingly, bank losses in the United States have been estimated to amount to over $2 billion per year [36]. However, the banking sector prefers not to report these losses due to the commercial sensitivities they perceive them [37]. This contributes towards the difficulty in establishing measures on the true cost of identity crime. The key issue this raises relates to the strength of responses which remain linked to the commensurate strength of that response [38].

Ultimately, there are costs related to identity crime, which are more easily identified, and those that are not, many of which are not considered in connection with one another.

IV. DEALING WITH IDENTITY CRIME AND SOCIAL NETWORKING

There are many practical difficulties in convicting identity criminals [39]. In the first place, in an international context, no central body is responsible for overseeing crime committed via the Internet or where on the Internet this crime might occur. Identifying and controlling crime perpetrated through social networking sites is fraught with difficulties [40]. The Internet is a dispersed communication entity that permeates country boundaries thereby making regulatory responses to crime difficult [40]. Further, different values influence the way in which crimes are viewed. Interpol increasingly plays a role in dealing with cybercrimes like identity crime by having a programme to deal with the emerging threats in this realm [41]. The Council of Europe Cybercrime Convention aims to harmonise the regulation of cyber-crimes [41]. It provides domestic criminal law authorities with the necessary cooperative mechanisms to investigate and prosecute computer crimes [41]. However, like most international instruments, crimes require attention through domestic laws [42]. Success will therefore be dependent on the stance maintained by each country in question.

The term ‘cybercrime’ has been used to describe crimes in which the computer or computer network is typically the target. This crime is distinguishable from other traditional crimes as it is limited to where the computer is used in the crime [43]. This thereby includes frauds in which the computer is used as a tool to commit the crime [43]. Likewise, if identity crime takes place through the use of a computer it is arguably included within the scope of the convention. However, the European Convention fails to deal directly with identity crime [44]. It captures computer-related forgery (article 7) as well as computer-related fraud (article 8) and thereby by association it would apply to related offences [45]. The significance of this is that the abovementioned convention would assist in the investigation and enforcement of identity crime despite not making reference to it [46]. In a global sense, unfortunately, there is nothing simple about applying criminal sanctions to international crimes like identity crime, particularly when they fall outside globally acknowledged atrocities such as genocide. Even so, the effectiveness of such responses is reliant on the preparedness of countries to agree and cooperate on responses to crime.

V. PRIVACY PERSPECTIVE

International responses to privacy share some of the challenges with the international regulation of crime. There is a lack of supremacy and centrality when it comes to the regulation of privacy internationally [46]. Akin to crime, domestic laws which are often based on international agreements are similarly relied upon to regulate privacy [47]. International principles of privacy protection are provided for in international agreements like the Universal Declaration of Human Rights [48]. These international agreements recognise the protection of the inalienable rights of all humans to privacy [48], highlighting the need for them to enjoy freedom of speech and belief [48]. Further, Article 12 suggests that no one should be subjected to interference with respect to their privacy [48]. Such international agreements have provided the foundation for the development of domestic laws [47]. Australia has been a member of the United Nations since 1945 [48] and has thereby developed such laws domestically. This can be seen in the Commonwealth Privacy Act, which provides for how information is collected, used and disclosed within Australia [49]. However, a limitation of the domestic privacy response in Australia is that it is not prescriptive and rather offers guidelines on the use of personal information. Further, it is constrained by the same jurisdictional boundaries that limit the extraterritorial reach of criminal sanctions explained above [50]. These are barriers to resolving the privacy-related issues of identity crime arising through the use of social networking.

VI. CHALLENGES IN DEALING WITH THE SOCIAL NETWORKING NEXUS WITH IDENTITY CRIME

A major challenge in responding to identity crime is the ability of law enforcement agencies to obtain evidence for the prosecution of this crime. The gathering of evidence on this crime involves obtaining digital evidence both on and off line [49]. It is essential for such investigative efforts across geographic borders to be effective as so much of crime such as identity crime takes place using the Internet, particularly due to the way in data are disseminated on social networking sites. The speed with which data transference takes place on the Internet makes the investigation of identity crimes difficult as the data possessed or used by a criminal can be destroyed or manipulated just as quickly [51]. Furthermore, as identity crime is cross jurisdictional then cooperation between law enforcement authorities is essential [52]. Any successful effort to investigate and enforce identity crime is reliant on the cooperation of countries [52] and the success of such efforts will also be dependent on the speed of such a response. In relation to civil responses to identity crime, there are similarly many barriers on the ability of the individual to successfully take civil action against the criminal as individuals have a greater scarcity of resources to successfully pursue such action. Similar issues around detecting and locating the offender exist for these actions also.

A key weakness in the integrity of data is the way in which individual users manage their own information. Users need to accept the need for greater accountability for the information shared on social networking sites. Each activity we engage in results in users leaving traces of themselves like digital footprints. Therefore, a commonsense response to dealing with the exploitation of social networking by identity criminals is for social networking users to improve their level of education about the relevant issues [49]. An educational program is necessary to ensure social networking users are both aware of the risks and of the need to exercise caution with respect to their personal information [53]. Moreover, in relation to the second point, this should take into account the ways in which, information might potentially be misused by identity criminals [54]. While education could have a direct impact on crime reduction [55] there will always typically be a proportion of the population not responsive to such efforts. The role of education is therefore not exhaustive but still should be regarded as another way of dealing with this crime. Social networking sites themselves should accept some responsibility in the protection of the user by encouraging the tacit sharing of personal information in some instances. This should be broader than the general technological security measures in place and needs to include the architecture underpinning the sites use [56]. This should involve reconsidering the ways in which, information sharing takes place on such sites and consideration of the architecture that facilitates this. Identity crime can be reduced through better understanding of and mitigation of these risks [57].

A number of additional and general technical responses can be applied to prevent identity crimes. The responses include improved measures of authentication and encryption, but are not limited to these [58]. The aim of such technological responses is to ensure data integrity is maintained while correspondingly preventing unwanted misuse of information or intrusion [59]. However, as with most responses, such efforts have vulnerabilities by way of the advancements criminals make to overcome them [59]. The strength of the responses to identity crime often needs to be balanced against the perceived costs of such preventative action [60]. Nevertheless, these responses provide additional ways of dealing with information security and thereby provide another way in which, identity crime can be responded to.

VII. Discussion

Ultimately, policymakers should consider a multi-faceted approach for dealing with identity crimes [61]. A mixture of techniques is necessary for counteracting the threats of this crime as the crime is ubiquitous response [62]. There are limitations with any approach to dealing with this crime, some of which have been discussed in this paper. The relationship of social networking and identity crime is unique and thereby requires creative responses. A major obstacle to responding to social networking and identity crime is the availability of accurate data relating to this relationship. While not all conceivable approaches to dealing with this phenomenon have been canvassed in this paper, the ones that have provide some insight into the many issues presented by this crime as well as some view of the plausible ways forward.

The information that is disseminated through the use of social networking is the key catalyst to identity crime which is largely based on the actions of individual users. The motivation for this research has been to explore the relationship between identity crime and social networking which has scarcely been explored in existing literature and to establish a basis upon which further research might take place. Further empirical research is needed to further probe the parameters of this relationship. It is hoped that through raising awareness of this relationship that further research interest is generated and that through further research, that social networking users will can take greater precautions to prevent themselves from becoming victims of this crime.

VIII. Evaluation

The material discussed in this paper, largely from secondary sources, identifies a relationship between social networking and identity crime. To further develop the contention, empirical research is needed to explore the scope of this relationship. In terms of the responses to this phenomenon, this paper has explored a number of technological and non-technological responses which are by no means exhaustive. Further research into the relationship between social networking and identity crime is likely to provide insights into the mechanisms that might better deal with this crime.

IX. Recommendations

Information is the vehicle to identity theft and considerable information is stored on social networking sites. Law and technological responses have limitations in relation to the extent they can mitigate this crime and particularly given the voluntary nature of information dissemination and the issues around jurisdiction and cooperation discussed. The individual vulnerability to this crime is through personal identification information which ultimately means that the behavioural factors are important to understanding the crime and indeed mitigating risk. Therefore, it is hoped that through the dissemination of research and information that individuals may become better informed of the risks inherent in the activities they engage with on the Internet: particularly social networking. Individual users of social networking need to take greater responsibility for the personal identification information shared on social networking sites to avoid victimisation. In this respect, if behavioural norms can be changed on social networking sites then the risk inherent with identity crime can be reduced.

X. Conclusion and future work

Social networking has encouraged many users to share personal information online, and social network users frequently engage in the sharing of information about themselves [9]. This article has considered the way in which social networking can potentially nourish the transference of personal information on the Internet, which in turn can provide identity criminals with the information needed to commit identity crime. While there are many ways to respond to this crime, a blend of techniques is likely to work best, given the pervasive nature of this crime and barriers presented by multiple jurisdictions. Future work is needed to explore these responses. An important starting point for dealing with this crime is to increase awareness of the risks associated with information sharing around social networking. If you have read this far, then this paper has achieved some of its educational aim: perhaps you will be more careful with your social networking profiles in the future. More research is needed to develop further knowledge about this crime and similarly more research is needed to understand the data surrounding identity crime and the nexus of this to the responses to it.

ACKNOWLEDGMENT

I would like to thank the support of The Business School at Federation University Australia (formerly University of Ballarat) which provided the assistance needed to prepare this article and Dr Ian Dobson for editorial support. I would also like to acknowledge the support of the institution I have studied in Australia and my research supervisors at Bond University.

REFERENCES

[1] J. B. Walther and S. Boyd, "Attraction to computer-mediated social support," in Communication Technology and Society: Audience Adoption and Uses, C. A. Lin and D. Atkin, Eds. Cresskill: Hampton Press, 2002, pp. 153-88.

[2] J. Bargh and K. McKenna. "The Internet and Social Life," Annual Review of Psychology, vol. 55, Feb. 2004, pp. 573-590, doi:10.1089/cpb.2005.8.423.

[3] I. Berson, M. Berson, and J. Ferron, "Emerging risks of violence in the digital age: Lessons for educators from an online study of adolescent girls in the United States," Journal of School Violence, vol. 1, Jan. 2002, pp. 51-71.

[4] P. Valkenburg and J. Peter, "Internet communication and its relation to well-being: Identifying some underlying mechanisms," Media Psychology, vol. 9, Dec. 2007, pp.23-58, doi:10.1080/15213260709336802.

[5] M.Green and T. Brock, "Antecedents and civic consequences of choosing real versus ersatz social activities," Media Psychology, vol. 11, Dec. 2008, pp. 566–592, doi:10.1080/15213260802491994.

[6] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns,"Computers in Human Behavior, vol. 25, Jan. 2009, pp. 153–160, doi>10.1016/j.chb.2008.08.006.

[7] F. Stajano and P. Wilson, "Understanding Scam Victims: Seven Principles for Systems Security," Communications of the ACM, vol. 54, Mar. 2011, pp. 70, doi :10.1145/1897852.1897872.

[8] A. Ledbetter, J. Mazer, J. DeGroot, K. Meyer, Y. Mao, and B. Swafford, "Attitudes toward online social connection and self-disclosure as predictors of Facebook communication and relational closeness," Communication Research, vol. 38, Feb. 2011, pp. 27–53, doi: 10.1177/0093650210365537.

[9] M. Lucas and N. Borrisov, "flyByNight: Mitigating the Privacy Risks of Social Netowrking," Proc. of the 7th ACM workshop on Privacy in the electronic society (WPES '08), ACM, Oct. 2008, pp. 1-8, doi>10.1145/1456403.1456405

[10] S. Hindujaa and J. Patchin, "Personal information of adolescents on the Internet: A quantitative content analysis of MySpace," Journal of Adolescence, vol. 31, Jan. 2008, pp. 125-146, doi:10.1016/j.adolescence.2007.05.004.

[11] N. Ellison, C. Steinfield, C, and Lampe. C, "Benefits of Facebook "friends:" Social capital and college students' use of online social network sites," Journal of Computer-Mediated Communication, vol. 12, Aug. 2007, pp.1143-1168, doi: 10.1111/j.1083-6101.2007.00367.x.

[12] Y. Yum and K. Hara, "Computer-mediated relationship development: A cross-cultural comparison," Journal of Computer-Mediated Communication, vol. 11, Aug. 2006, pp. 133–152, doi: 10.1111/j.1083-6101.2006.tb00307.x.

[13] P. Van Eecke and M. Truyens, "Privacy and social networks," Computer Law & Security Review, vol. 26, Sept. 2010, pp. 535-546, doi: http://dx.doi.org/10.1016/j.clsr.2010.07.006.

[14] H. Jelicic, D. Bobek, E. Phelps, and R. Lerner, "Using positive youth development to predict contribution and risk behaviors in early adolescence: Findings from the first two waves of the 4-H Study of Positive Youth Development," International Journal of Behavioral Development, vol. 31, May. 2007, pp. 263–273, doi: 10.1177/0165025407076439.

[15] J. Huang, D. Jacobs, D. Derevensky, J. Gupta, R, and T. Paskus, "Gambling and health risk behaviors among US college student-athletes: Findings from a national study," Journal of Adolescent Health, vol .40, May. 2007, pp. 390-397, doi:10.1016/j.jadohealth.2006.11.146.

[16] K. Saunders and B. Zucker, "Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act," Cornell Journal of Law and Public Policy, vol. 8, Spring. 1999, pp.661.

[17] T. Hemphill, "Identity Theft: A Cost of Business?," Business and Society Review, vol. 106, Dec. 2001, pp.51-63, doi:10.1111/0045-3609.00101.

[18] N. Archer, S. Sproule, Y. Yuan, K. Guo, and J. Xiang, Identity Theft and Fraud Evaluating and Managing Risk. Ottawa, Canada: University of Ottawa Press, 2012.

[19] Australian Crime Commission. (2009, November, 28). Organised Crime in Australia 2011. [Online]. Available: http://www.crimecommission.gov.au/sites/default/files/files/OCA/2011/oca2011.pdf [retrieved: January, 2011].

[20] United Kingdom Cabinet Office. (2002, February 15). Identity Fraud: A Study. [Online]. Available: http://www.statewatch.org/news/2004/may/id-fraud-report.pdf [retrieved: November, 2013].

[21] International Civil Aviation Organization. (2009, November, 9). Towards Better Practice in National Identity Management. [Online]. Available: http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-19/TagMrtd19-wp03.pdf [retrieved: October, 2013].

[22] Government of South Australian (2005, May.). Australian E-Commerce Safety Guide 2005. [Online]. Available: http://www.cbs.sa.gov.au/assets/files/EcommGuide_2005.pdf [retrieved: September, 2013].

[23] L. Langton, M. Planty, and US Department of Justice (2008, Dec.). Victims of Identity Theft, 2008 [Online]. Available: http://bjs.ojp.usdoj.gov/content/pub/pdf/vit08.pdf [retrieved: December, 2010].

[24] Carnegie Mellon. (2011, Mar.). Child Identity Theft. 2011 [Online]. Available: http://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf [retrieved: March, 2011].

[25] S. Willis and B. Tranter, "Beyond the "Digital Divide": Internet Diffusion and Inequality in Australia," Journal of Sociology, vol. 42, Mar. 2006, pp. 43-59, doi:10.1177/1440783306061352.

[26] L. Plowman, O. Stevenson, C. Stephen, and J. McPake, "Preschool children's learning with technology at home," Computers & Education, vol. 59, Aug. 2012, pp. 30-37, doi:http://dx.doi.org/10.1016/j.compedu.2011.11.014.

[27] S. Livingstone and E. Helsper, "Parental mediation and children's Internet use," Journal of Broadcasting and Electronic Media, vol. 52, Dec. 2008, pp. 581–599, DOI: 10.1080/08838150802437396.

[28] Australian Government. (2013, Feb.). Identity Theft. [Online]. Available: http://www.scamwatch.gov.au/content/index.phtml/tag/identitytheft [retrieved: March 2011].

[29] National Crime Justice Reference Service. (2013, Jan.). Identity Theft – Facts and Figures. [Online]. Available: https://www.ncjrs.gov/spotlight/identity_theft/facts.html [retrieved: October, 2013].

[30] Australian Bureau of Statistics. (2012, Apr.). Personal fraud costs Australians $1.4 billion. [Online]. Available: http://www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbytitle/B634CE9C7619C801CA25747400263E7E?OpenDocument [retrieved: April, 2012].

[31] Australian Bureau of Statistics. (2012, Apr.). Personal Fraud 2010-2011. [Online]. Available: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/65767D57E11FC149CA2579E40012057F?opendocument [retrieved: November, 2013].

[32] CIFAS. (2012, Jun.). Is Identity Fraud Serious? [Online]. Available: http://www.cifas.org.uk/is_identity_fraud_serious [retrieved: October, 2013].

[33] R. Smith. (2003, Sep.). Addressing Identity-Related Fraud. Presented at Cards Australasia. [Online]. Available: http://www.aic.gov.au/about_aic/research_programs/staff/~/media/conferences/other/smith_russell/2003-09-identity.ashx [retrieved: December, 2012].

[34] M. Perl, "It's Not Always About the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft," Journal of Criminal Law and Criminology, vol. 94, Fall. 2003, pp.169-208.

[35] D. Lacey and S. Cuganesan, "The Role of Organizations in Identity Theft Response: The Organization-Individual Victim Dynamic," The Journal of Consumer Affairs, vol. 38, Jul. 2004, pp 244-261, doi:10.1111/j.1745-6606.2004.tb00867.x.

[36] Kroll Advisory Solutions (2011, May.). Global Fraud Report: The Strategic Impact of Fraud, Regulation, and Compliance [Online]. Available: http://www.krollconsulting.com/media/pdfs/KRL_FraudReport2011.pdf [retrieved: December, 2013].

[37] Federal Trade Commission (2003, Sep.). Identity Theft Survey Report Federal Trade Commission [Online]. Available: http://www.ftc.gov/os/2003/09/synovatereport.pdf [retrieved: December, 2013].

[38] Pat Mayhew and Australian Institute of Criminology (2003, Apr.). Counting the Costs of Crime in Australia [Online]. Available: http://www.aic.gov.au/documents/A/A/3/%7BAA329573-5D62-46FB-9E6F-4D86A6DDD9BC%7Dti247.pdf [retrieved: November, 2013].

[39] R. Smith. (2002, Jul.). Examining the Legislative and Regulatory Controls on Identity Fraud in Australia [Online]. Available: http://www.aic.gov.au/media_library/conferences/other/smith_russell/2002-07-fraud.pdf [retrieved: November, 2012].

[40] B. Fitzgerald, A. Fitzgerald, T. Beale, Y. Lim, and G. Middleton, Internet and C-Commerce Law: Technology, Law and Policy. Pyrmont: Lawbook Co, 2007.

[41] Interpol (2014, Jan.). Interpold [Online]. Available: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [retrieved: Jan, 2014].

[42] S. Brenner, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law," Murdoch University Electronic Journal of Law, vol. 8, Jun. 2001, pp. 1.

[43] J. Clough, "The Council of Europe Convention on Cybercrime: Defining 'Crime' in a digital world," Criminal Law Forum, vol. 23, Dec. 2012, pp. 363-391, doi:10.1007/s10609-012-9183-3.

[44] M. Gercke and Council of Europe. (2007, Nov.). Internet-Related Identity Theft Discussion Paper. [Online]. Available: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf [retrieved: January, 2014].

[45] Council of Europe. (2011, Jul.). Convention on Cybercrime: Member States of the Council of Europe – Article 12 [Online]. Available: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG [retrieved: January, 2014].

[46] K. Grewlich, Governance in 'Cyberspace' Access and Public Interest in Global Communications, Boston, USA: Klewer Law International, 1999.

[47] International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

[48] Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948).

[49] Australian Government: Office of the Australian Information Commissioner. (2007, Aug.). Scanning "Proof of Identity" Documents [Online]. Available: http://www.privacy.gov.au/materials/types/infosheets/view/6553 [retrieved: December, 2013].

[50] P. Argy, "Internet Content Regulation: an Australian Computer Society Perspective," University of New South Wales Law Journal, vol. 23, Jul. 2000, pp. 265-267.

[51] C. Blakesley, "United States Jurisdiction over Extraterritorial Crime," The Journal of Criminal Law and Criminology, vol. 73, Jan. 1982, pp.1109.

[52] A. Cassese, International Law. Kansas, USA: Oxford University Press, 2001.

[53] Organisation for Economic Co-operation and Development. (2008, Jun.). OECD Policy Guidance on Online Identity Theft [Online]. Available: http://www.oecd.org/dataoecd/49/39/40879136.pdf [retrieved: October, 2013].

[54] M. Harer and Federal Bureau of Prisons. (1994, Aug.). Recidivism among Federal Prisoners Released in 1987 [Online]. Available: http://149.101.37.70/news/research_projects/published_reports/recidivism/oreprrecid87.pdf [retrieved: October, 2013].

[55] Parliament of Australia - House of Representatives Standing Committee on Communication (2010, Jun.). Chapter 6: Criminal and Law Enforcement Framework [Online]. Available: http://parlinfo.aph.gov.au/parlInfo/search/summary/summary.w3p;adv=yes;orderBy=customrank;page=0;resCount=Default;query=Criminal+and+Law+Enforcement+Framework [retrieved: April, 2013].

[56] B. Schneier, Secrets and Lies: Digital Security in a Networked World. New York, USA: John Wiley, 2000.

[57] L. Lessig, Code and Other Laws of Cyberspace. Virginia, USA: Basic Books, 1999.

[58] J. Lynch, “Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks,” Berkeley Technology Law Journal, vol. 20, Jan. 2005, pp. 266-67.

[59] R. Sullivan, “Can Smart Cards Reduce Payments Fraud and Identity Fraud,” Economic Review, vol. 93, 2008, pp. 36-62.

[60] N. Phair, Cybercrime: the Reality of the Threat. Kambah, ACT: E-Security Publishing, 2007.

[61] G. Newman, “Policy Thoughts on “Bounded Rationality of Identity Thieves,”' Criminology & Public Policy, vol. 271, Jun. 2009, pp.271-278, doi: 10.1111/j.1745-9133.2009.00562.x.

[62] R. G. Broadhurst and P. N. Grabosky, “Computer-Related Crime in Asia: Emergent Issues,” in Cyber-Crime: The Challenge in Asia, R. G. Broadhurst and P. N. Grabosky. Eds. Hong Kong: Hong Kong University Press, 2005, p 1.

Detecting New Concepts in Social Media using Co-burst Pattern Mining

Takako Hashimoto*, David Shepard†, Basabi Chakraborty‡ and Tetsuji Kuboyama§
*Commerce and Economics, Chiba University of Commerce, Chiba, Japan
Email: takako@cuc.ac.jp
†Center for Digital Humanities, University of California, Los Angeles, USA
Email: shepard.david@gmail.com
‡Software and Information Science, Iwate Prefectural University, Japan
Email: basabi@iwate-pu.ac.jp
§Computer Centre, Gakushuin University, Japan
Email: kuboyama@tk.cc.gakushuin.ac.jp

***Abstract*—This paper proposes a method for detecting new concepts in social media using co-burst pattern mining technique. The new concepts are defined as correlations between unexpected words. The target social media are viewers' comments attached to web videos and Twitter's tweets related to the East Japan Great Earthquake that happened on Mar. 11 in 2011. Our proposed method first crawls viewers' comments from web videos, and extracts words from them. Then it selects motive words candidates from words, and counts the occurrence numbers of tweets that include motive words candidates. To detect new concepts, it generates burst patterns based on occurrence numbers of motive words candidates over time and detects unexpected correlations between motive words candidates. By our method, after the earthquake, new unexpected correlations between motive words in social media are recognized as new concepts. For example, the method could extract motive words from web video comments, such as "escape, nuclear plant" and "Tokyo Electric Power Co., Inc.(TEPCO, that owns the nuclear plant), president." Then it could detect the new concept "escape (from) nuclear plant" and "TEPCO's president" on Twitter. In this paper, we provide the preliminary approximation results and discuss the effectiveness of our proposed method.**

Keywords*—*Social meda, burst pattern, unexpected words' correlation, video service, Twitter, East Japan Great Earthquake.

I. Introduction

Social media in which individual users post their opinions and gradually build new concepts together, is recognized as one of the important collaborations in today's information oriented society. After the East Japan Great Earthquake, we could detect discussions related to the nuclear plant, Tokyo Electric Power Company (TEPCO) and so on, that could not be recognized before the earthquake. We defined new concepts as correlations between unexpected words that could not be recognized before the earthquake, such as "nuclear plant, escape" and "TEPCO, president." Exploring newly-built concepts over time on social media is significant, so that we believe we can gain a rich insight into social context.

We already proposed the graph-based topic extraction method [1] using the modularity measure [2]. We also proposed an approach to extract hidden topics over time from social media messages using the latent semantic analysis (LSA) technique [3] , [4]. Our previous work targeted single social media such as a blog or a buzz marketing site. However, new concepts are sometimes created triggered by mutual relationships between different social media. This paper targets multiple social media and proposes the method to explore new concepts by analyzing multiple social media. The target social media are web video comments and tweets related to the East Japan Great Earthquake. Our proposed method first crawls viewers' comments attached to web videos, and extracts words from them. It selects motive words candidates from extracted word, and then counts the occurrence numbers of tweets that include the motive words candidates in Twitter. To detect new concepts, it generates burst patterns based on occurrence numbers of motive words candidates over time and analyzes burst correlations between them. By our method, new burst correlations between motive words triggered by social media are recognized as new concepts. For example, after the earthquake, we could extract "escape, nuclear plant" as motive words from web video comments, and detect the new concept "escape (from) nuclear plant" on Twitter.

The contributions of this paper are as follows:

- Propose the method for detecting new concepts from mutual correlation of multiple social media (cross-media analysis)
- Show concrete examples for new concepts that appeared after the East Japan Great Earthquake

This paper is organized as follows. Section II refers to existing researches. Section III introduces our target social media. Section IV illustrates our proposed method to explore new concepts by analyzing relationships between different social media. Section V shows the preliminary approximation result of our method that targets web video comments and tweets related to the East Japan Great Earthquake. Finally, Section VI concludes this paper.

II. Related Work

Most related works for detecting topics/concepts focus on single media, such as blogs, Twitter, and web videos respectively. Sekiguchi *et al.* [5] treated recent blogger posts and analyzed the word co-occurrence and the repeating rate of word. They visualized the relation between words and showed topics in social media through the visualization results. Asur *et al.* [6] investigated trending topics on Twitter. They proposed a simple model based on the number of tweets and found that the resonance of the content with the users of the social network plays a major role in causing trends. Liu *et al.* [7] and Cao *et al.* [8] focus on web video analysis. Especially, Cao *et al.* [8] clusters video tags into groups to get small events and then link these events into topics based on textual and video similarity. On the other hand, our proposed method focuses on multiple social media and analyzes them. It can flexibly show concepts transition by taking into cross-media over time.

As for cross-media analysis, most existing works focus on co-clustering among multiple social media. Xue *et al.* [9] proposed the cross-media topic detection method that was based on co-clustering and detect new topics. Our proposed method focuses on characteristic words extracted from social media and then detect co-occurrence patterns among them that can be recognized as new concepts.

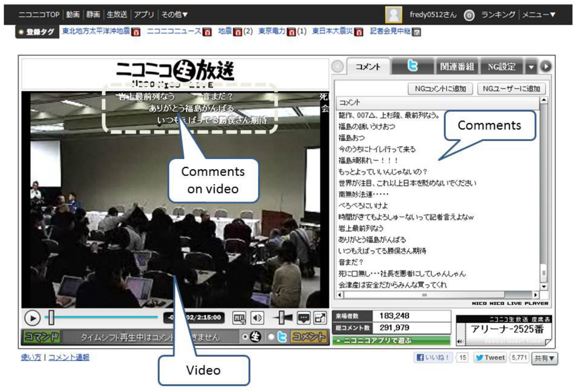
Regarding research on detecting temporal relations, Radinsky *et al.* [10] proposed Temporal Semantic Analysis (TSA), a semantic relatedness model, that captures the words' temporal information. They targeted words in news archives (New York Times, etc.) and used the dynamic time warping technique to compute a semantic relation between pre-defined words. Wang *et al.* [11] proposed time series analysis which has been used to detect similar topic patterns. They focus on specific burst topic patterns in coordinated text streams and try to find similar topics. Zhou *et al.* [12] addressed the community discovery problem in a temporal heterogeneous social network of published documents over time. They showed temporal communities by threading the statically derived communities in consecutive time periods using a new graph partitioning algorithm. Qiu *et al.* [13] focused on the problem of discovering the temporal organizational structure from a dynamic social network using a hierarchical community model. The above existing methods focused on single media and analyzed their transition. In our method, on the other hand, new concepts exploration can be analyzed by investigating multiple social media over time based on co-burst pattern of characteristic words.

III. Target Social Media

The aim of our proposed method is cross-media concepts detection, so that it targets multiple social media. As the first targets, Nicovideo and Twitter have been selected in our work.

A. Nicovideo comments related to the East Japan Great Earthquake

Nicovideo is one of the most popular video sharing web sites in Japan [14]. In Nicovideo, users can upload, view and share videos, and also add comments while watching videos. Unlike other video sharing sites, comments are overlaid directly onto the video, synchronized to a specific playback time. Users can communicate each other through video comments and a sense of a shared watching experience could be created. After the East Japan Great Earthquake, Nicovideo provided live programs like the government press conferences, TEPCO press conferences and so on (Figure 1).



岩上最前列なう　音まだ？
ありがとう福島がんばる
いつもえばってる勝俣さん期待

コメント
龍作、007△、上杉隆、最前列なう。
福島の誠いうけおつ
福島おつ
今のうちにトイレ行って来る
福島頑張れー！！！
もっとよっていいんじゃないの？
世界が注目、これ以上日本を貶めないでください
南無妙法連・・・・
べろべろにいけよ
時間がきてもよろしゅーないって記者言えよなw
岩上最前列なう
ありがとう福島がんばる
いつもえばってる勝俣さん期待
音まだ？
死に口無し・・・社長を悪者にしてしゃんしゃん
会津産は安全だからみんな買ってくれ

Fig. 1. An example of Nicovideo.

These live programs were not provided by major TV broadcasting companies and viewers could get actual information that they could not watch through mayor TV programs. Users' comments that were attached to the live program could be a trigger to produce new concepts related to the earthquake among users, and the concepts had an influence on users' behavior. Hence, the video sharing website may lead opinions in society. By analyzing comments on Nicovideo, we expect that the relationships between Nicovideo and other social media can be detected and the new concepts propagation can be illustrated.

B. Twitter's tweets related to the East Japan Great Earthquake

Tweets related to the East Japan Great Earthquake is also targeted in this paper. During the earthquake, people tweeted a lot of things about concerns for affected people and disaster situation, fear for future and so on (Table I).

TABLE I. Example of tweets related to the East Japan Great Earthquake.

Date	*Tweet (translated into English)*
2011/03/11	I can not contact my parents who live in Miyagi. #jishin, #miyage
2011/03/11	Be strong, we are with you #jishin
2011/03/11	The JR train service has returned to normal.. #jishin
2011/03/12	The government press conference has just started. #jishin#nhk
2011/03/12	My friend was almost to get robbed. Please take care.. #jishin

The social media monitoring company Hottolink [17] tracked users who used one of 43 hashtags (for example, #jishin, #nhk, and #prayforjapan) or one of 21 keywords related to the disaster. Later, they captured all tweets sent by all of these users between Mar. 9th and Apr. 2nd. This resulted in an archive of around 200 million tweets, sent by around 1 million users. Capturing programs searched tweets by hashtag, consequently, and many of these tweets contain useful information about users responses to the disaster. These tweets are one of big data and it is significant to analyze them to detect new concept generated after the quake.

IV. Proposed Method for Detecting New Concepts in Social Media using Co-burst Pattern Mining

Our proposed method focuses on detecting new concepts in social media. We define a new concept as new words' burst correlation. Suppose there are two words like "president" and "Tokyo Electric Power Co., Inc.(TEPCO, that owns the nuclear plant)." Before the East Japan Great Earthquake, we did not have the special meaning between "president" and "TEPCO," so that the correlations between "president" and "TEPCO" could not be recognized. But after the press conference by TEPCO, we suddenly began to have the new meaning of "president" and "TEPCO" as the person who was accountable for the nuclear accident. Actually, we could find new co-occurring patterns between "president" and "TEPCO" in Twitter. Our hypothesis is that new concepts are suddenly generated by communications in social media, and propagated quickly in social media. Hence, the objective of our method is to find new motive words candidates that can be basis of new concepts, and detect new correlations between them in social media.

There are two types of social media in our method. One generates motive words, and the other propagates motive words correlation (new concepts). As the social media for motive words generation (TriggerSM) and the social media for words correlation propagation (PropagateSM), in this paper, we use Nicovideo and Twitter respectively.

Our method consists of the following 3 steps.

Step A: Find motive word candidates from TriggerSM.
Step B: Count occurrence numbers of motive words candidates in PropagateSM.
Step C: Analyze time series motive words' co-occurring patterns and detect new concepts on PropagateSM.

Figure 2 illustrates our proposed method's steps.

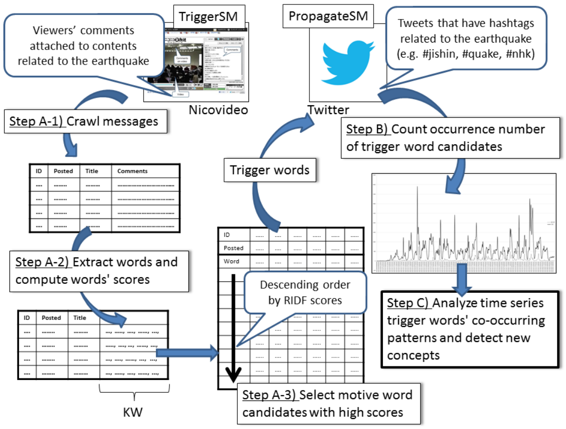

TriggerSM
Viewers' comments attached to contents related to the earthquake
Nicovideo
PropagateSM
Tweets that have hashtags related to the earthquake (e.g. #jishin, #quake, #nhk)
Twitter
Step A-1) Crawl messages
ID
Posted
Title
Comments
Step A-2) Extract words and compute words' scores
ID
Posted
Title
KW
Trigger words
ID
Posted
Word
Descending order by RIDF scores
Step A-3) Select motive word candidates with high scores
Step B) Count occurrence number of trigger word candidates
Step C) Analyze time series trigger words' co-occurring patterns and detect new concepts

Fig. 2. Proposed method.

The following is the description of each step.

A. Find motive word candidates from TriggerSM.

This step consists of the following 3 sub-steps.

1) Crawl messages from TriggerSM.
2) Extract words candidates and compute their scores.
3) Select motive words candidates with high scores.

Each sub-step is explained in the following:

1) Crawl messages from TriggerSM: This sub-step crawls messages from TriggerSm. The target social media is viewers' comments attached to Nicovideo live contents (the press conferences related to the East Japan Great Earthquake). A set of comments attached to one video content were recognized as one document d_i as the following tuples:

$$d_i = (MID_i, Posted_i, Title_i, Content_i) \tag{1}$$

Here, MID_i is an ID of each document, $Posted_i$ is a broadcast date-time that the document (content), $Title_i$ is a title of each document (content) and $Content_i$ is a combined text of video comments. Table II shows some example of d_i.

TABLE II. Example of d_i.

MID	$Posted_i$	$Title_i$	$Content_i$
1	2011/03/11	Press Conference by Government	I can not believe, we should send something to affected people, It is really dangerous., ...
2	2011/03/14	Press Conference by TEPCO	The president should take responsibility, Where is the president? The vice president is also wired, ...
3	2011/03/15	Press Conference by TEPCO	The nuclear plant is really bad, melt down?, TEPCO is untrustworthy, ...

2) Extract words candidates and compute their scores: This sub-step extracts words that are nouns, verbs, adjectives, and adverbs from $Content_i$ of each d_i by morphological analysis. We use Mecab that is yet another Japanese Dependency Structure Analyzer [19] for word extraction. Then, the score of an individual word in d_i is calculated using RIDF [20] measure that is based on the poison distribution. We form a list of keywords $KW = \{kw_i\}$.

$$kw_i = (MID_i, Posted_i, \{w_{ij}, v_{ij}\}) \tag{2}$$

Here, $\{w_{ij}, v_{ij}\}$ is a list of a pair that consists of an extracted word w_{ij} from document d_i, and the corresponding RIDF value v_{ij} of w_{ij}.

3) Select motive word candidates according to their scores.: This sub-step sorts $\{w_{ij}, v_{ij}\}$ in descending order by v_{ij}. Then the step analyzes KW over time and finds newly appeared words that are high on the list $\{w_{ij}, v_{ij}\}$ of each kw_i. We focus on top n words of each kw_i and among those, we find characteristic words that did not seem appear before the earthquake as motive words candidates.

B. Count occurrence numbers of motive words candidates in PropagateSM

Then the method counts time series occurrence numbers of candidates words in PropagateSM. The occurrence number is counted before and after the earthquake. If the occurrence number of the word is low before the quake, and becomes high after the quake, the word can be recognized to become burst after the quake.

C. Analyze time series motive words' co-occurring patterns and detect new concepts on PropagateSM.

The method checks the time series burst pattern for each motive word candidate from the occurrence number of each word. To detect the burst pattern, we adopt the method proposed by Zhu *et al.* [18]. Zhu *et al.* proposed the burst detection method using elastic windows over time. They propose the shifted wavelet tree as the data structure for efficient burst monitoring, so that their method can detect burst flexibly. The shifted wavelet tree uses the adjacent windows of the same level are half overlapping (Figure3). These additional windows provide valuable overlapping information for the time series. It will be better to analyze co-burst patterns between words than the conventional wavelet tree.

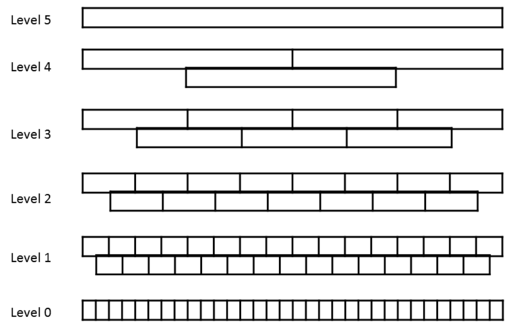


Fig. 3. Shifted Wavelet Tree proposed by Zhu *et al.*.

Any subsequence with length $w, w \leq 2^i$ is included in some subsequence(s) with length 2^i, and therefore is included in one of the windows at level $i+1$. We say that windows with size $w; 2^{i-1} \leq w \leq 2^i$, are monitored by level $i+1$ of the SWT.

The method computes the coefficient of correlation between burst patterns of motive words candidates. If the coefficient of correlation is larger than the threshold γ, the new concept is supposed to be generated.

V. Preliminary Approximation

We crawled around 94000 viewers' comments attached to 67 live videos (broadcasted from Mar. 13 to 24 in 2011) related to the East Japan Great Earthquake in Nicovideo (TriggerSM). Then words were extracted from crawled comments and the RIDF score for each word was computed. Table III shows some example of documents $\{d_i\}$ x words $\{w_{ij}\}$ matrix with the RIDF scores.

Then $\{w_{ij}\}$ in d_i were sorted in descending order by $\{v_{ij}\}$. We set $n = 10$, and top 10 words with high RIDF value in each d_i were extracted. Table IV shows some example of extracted top 10 words for each d_i.

TABLE III. Example of $\{d_i\} - words\{w_{ij}\}$ matrix.

MID	$Posted_i$	escape	JSDF [15]	life	publish	president	...
1	2011/03/13 20:00	0	0	0	0	0.1	...
2	2011/03/15 8:30	0.027	0.026	0.013	0.01	0.11	...
3	2011/03/15 14:00	0	0	0	0	0.01	...
4	2011/03/15 21:00	0	0.01	0.01	0	0.03	...
5	2011/03/15 23:30	0.02	0.01	0.01	0	0.01	....
6	....	....	....	....	....	....	....

TABLE IV. Example of trigger words with high RIDF values in $\{d_i\}$.

MID	1	2	3	4	...	21	...
$Date_i$	$3/13$ 20:00	$3/15$ 8:30	$3/15$ 14:00	$3/15$ 21:00	... ...	$3/16$ 18:00	... ...
#1	blackout	ask	conference	blackout	...	vice-president	...
#2	TEPCO	Fukushima	NISA[16]	TEPCO	...	nuclear-plant	...
#3	press	president	TEPCO	nuclear-plant	...	president	...
#4	escape	escape	rain	NISA	...	TEPCO	....
#5	stop	nuclear-plant	field	electricity	...	measures	....
#6	president	planned-outrage	mass-media	conference	...	TEPCO	....
#7	measures	JSDF	measures	no-problem	...	problem	....
#8	fire-fighting	TEPCO	cover-up	power-saving	...	electricity	....
#9	Fukushima	field	officer	time	...	field	....
#10	nulcear-plant	fix	nuclear-plant	affected	...	remote	....

For example, in the document of $MID = 1$, words such as ”blackout”, ”TEPCO”, ”press”, ”escape”, ”stop” and ”president” were listed up. In the document of $MID = 6$, words such as ”president”, ”planned-outrage”, ”mass-media”, ”TEPCO”, ”conference” and ”TEPCO” were listed up. These words that characterize contents were recognized as trigger words candidates.

In this paper, we defined the follwoing 23 words as trigger words candidates.

”planned-outrage”, ”blackout”, ”field”, ”Edano”, ”JSDF”, ”employee”, ”fire-fighting”, ”government”, ”Shimizu”, ”power-saving”, ”measures”, ”stop”, ”power”, ”escape”, ”NISA”, ”radioactivity”, ”nuclear plant”, ”officer”, ”TEPCO”, ”Fukushima”, ”president”, ”vice-president”, ”director”

As for above trigger words candidates, we counted occurrence number of each candidate in Twitter data (from Mar. 9 to Apr. 2) provided by Hottolink [17]. Figure 4 and Figure 5 show some result of the occurrence number of each trigger word candidate.

In Figure 4, we can not find the explicit correlation between the occurrence pattern between president, vice-president and director in Twitter. On the other hand, in Figure 5, the occurrence pattern between nuclear plant and Fukushima in Twitter seems strongly co-related. Actually, ”Fukushima nuclear plant” became the general word after the quake, so that these words must be co-related. However, correlations between other words were unexpected. To analyze correlations precisely, co-burst patterns were considered.

Then, we adopt the burst detection method proposed by Zhu *et al.* [18] to analyze co-burst patterns between trigger words candidates. Figure 6 shows results of burst patterns of trigger words candidates. The horizontal axis shows time (from Mar. 9 to Apr. 2), and black cells indicate burst periods for each word Figure 7 shows correlations between burst patterns of trigger words. We set the threshold value γ as 0.5 and the correlations larger than the threshold are shown by shaded region.

According to Figure 7, we could observe the following unexpected concepts

- escape → Fukushima, nuclear-plant
- TEPCO → president, vice-president, director, employee
- firefighting → power, JSDF, radioactivity, nulcear-plant
- measures → nuclear-plant, power, radioactivity, Fukushima

We could find the new concepts such as ”escape (from) Fukushima”, ”TEPCO president/vice-president/... (for condemnation)” ”(new relationships between) firefighting, power, JSDF, radioactivity, and nulcear-plant”, and ”(the importance of) measures for nuclear-plant, power, radioactivity and Fukushima.”

VI. Conclusion

This paper proposed the method to detect new concepts in multiple social media after the topical problem like the East Japan Great Earthquake. As the preliminary approximation result, after the East Japan Great Earthquake, from web video service (Nicovideo) and Twitter, new concepts could be detected and shown as unexpected words co-occurrences. For example, after the earthquake, new concepts for the nuclear plant, TEPCO, and so on were recognized on social media.

As the future work, we plan to improve the method for automatically selecting trigger words candidates, and analyze the time series concepts detection using the video time line. Moreover, the method should be applied to other data and evaluated compared to the conventional method such as wavelet tree. As the future work, we are going to improve the technique for trigger words candidates selection and focus on precisely analyzing burst patterns over time using the time line of the video. In addition, we will improve the method by considering scalability.

References

[1] T. Hashimoto, T. Kuboyama, B. Chakraborty, and Y. Shirota, Discovering Topic Transition about the East Japan Great Earthquake in Dynamic Social Media, GHTC 2012, Oct. 2012, pp. 259-264.

[2] M. E. J. Newman, Modularity and community structure in networks, National Academy of Science USA 103(23), 2006, pp. 8577-8696.

[3] T. K. Landauer and S. T. Dumais, A solution to Plato’s problem: The latent semantic analysis theory of the acquisition, induction, and representation of knowledge, Psychological Review, 104(2), 1997, pp. 211-240.

[4] T. Hashimoto, B. Chakraborty, T. Kuboyama, and Y. Shirota, Temporal Awareness of Needs after East Japan Great Earthquake using Latent Semantic Analysis, EJC2013 (the 23nd European-Japanese Conference on Information Modelling and Knowledge Bases), Jun. 2013, pp.214-226.

[5] Y. Sekiguchi, H. Kawashima, and T. Uchiyama, Discovery of related topics using series of blogsites’ entries, JSAI 2008, 2I1-1, 2008 (in Japanese).

[6] S. Asur, B.A. Huberman, G. Szbaó, and C. Wang, Trends in social media: Persistence and decay, ICWSM 2011, Jul. 2011, pp. 434-437.

[7] L. Liu, L. Sun, Y. Rui, Y. Shi, and S. Yang, Web video topic discovery and tracking via bipartite graph reinforcement model, IWWWC 2011, Apr. 2011, pp. 1009-1018.

[8] J. Cao, C. W. Ngo, Y. D. Zhang, and J. T. Li, Tracking web video topics: discovery, visualization and monitoring, IEEE Transactions on Circuits and Systems for Video Technology 21(12), 2011, pp. 1835-1846, 2011.

[9] Z. Xue, Z. Jiang, G. Li, and Q. Huang, Cross-media topic detection associated with hot search queries, ICIMCS 2013, Aug. 2013, pp. 403-406.

[10] K. Radinsky, E. Agichtein, E. Gabrilovich, and S. Markovitch, A word at a time: Computing word relatedness using temporal semantic analysis, WWW 2011, Mar. 2011, pp. 337-346.

[11] X. Wang, C. Zhai, X. Hu, and R. Sproat, Mining correlated bursty topic patterns from coordinated text streams, KDD 2007, Aug. 2007, pp. 784-793.

[12] D. Zhou, I. Councill, H. Zha, and C. L. Giles, Discovering temporal communities from social network documents, ICDM 2007, Oct. 2007, pp. 745-750.

[13] J. Qiu, Z. Lin, C. Tang, and S. Qiao, Discovering organizational structure in dynamic social network, ICDM 2009, Dec. 2009, pp. 932-937.

[14] Nicovideo, [Online]. Available: http://www.nicovideo.jp/, [retrieved: Jan., 2014]

[15] JSDF, [Online]. Available: Japan Self-Defense Forces, http://www.mod.go.jp/asdf/English_page/, [retrieved: Jan., 2014]

[16] NISA, [Online]. Available: Nuclear and Industrial Safety Agency, http://www.nsr.go.jp/archive/nisa/english/, [retrieved: Jan., 2014]

[17] Hottolink,Inc., [Online]. Available: http://hottolink.co.jp, [retrieved: Jan., 2014]

[18] Y. Zhu and D. Shasha, Efficient elastic burst detection in data streams KDD 2003, Aug. 2003, pp. 336-345.

[19] T. Kudo, MeCab : Yet Another Part-of-Speech and Morphological Analyzer, [Online]. Available: http://mecab.sourceforge.net/, [retrieved: Jan., 2014]

[20] K. W. Church and W. A. Gale, Poisson mixtures, Natural Language Engineering **1**, 1995, pp. 163–190.

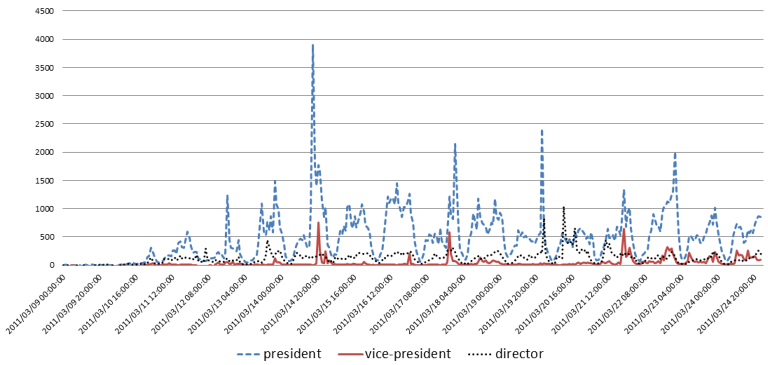


Fig. 4. Occurrence number of president, vice-president and director in Twitter

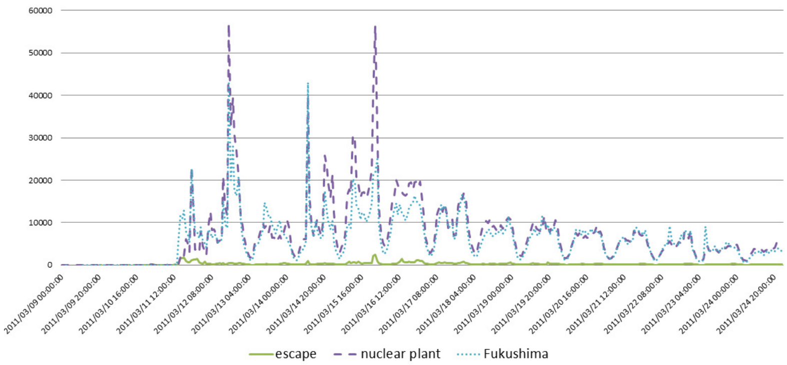


Fig. 5. Occurrence number of escape, nuclear plant and Fukushima in Twitter

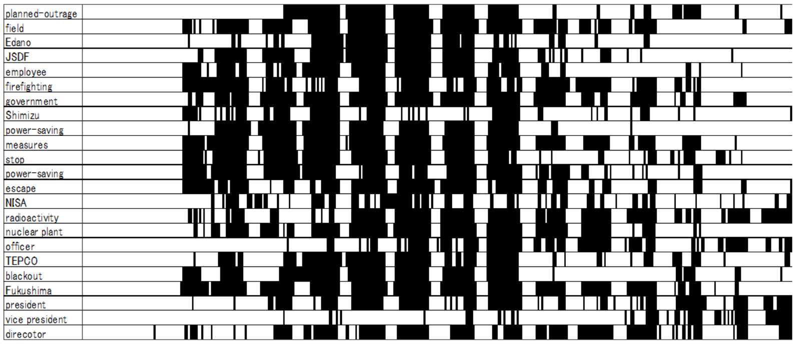
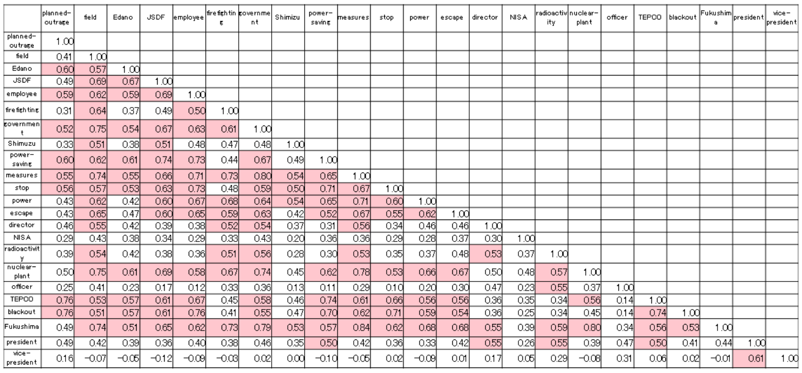


Fig. 6. Burst patterns of trigger words candidates



	planned-outrage	field	Edano	JSDF	employee	firefighting	government	Shimizu	power-saving	measures	stop	power	escape	director	NISA	radioactivity	nuclear-plant	officer	TEPCO	blackout	Fukushima	president	vice-president
planned-outrage	1.00																						
field	0.41	1.00																					
Edano	0.60	0.57	1.00																				
JSDF	0.49	0.69	0.67	1.00																			
employee	0.59	0.62	0.59	0.69	1.00																		
firefighting	0.31	0.64	0.37	0.49	0.50	1.00																	
government	0.52	0.75	0.54	0.67	0.63	0.61	1.00																
Shimuzu	0.33	0.51	0.38	0.51	0.48	0.47	0.48	1.00															
power-saving	0.60	0.62	0.61	0.74	0.73	0.44	0.67	0.49	1.00														
measures	0.55	0.74	0.55	0.66	0.71	0.73	0.80	0.54	0.65	1.00													
stop	0.56	0.57	0.53	0.63	0.73	0.48	0.59	0.50	0.71	0.67	1.00												
power	0.43	0.62	0.42	0.60	0.67	0.68	0.64	0.54	0.65	0.71	0.60	1.00											
escape	0.43	0.65	0.47	0.60	0.65	0.59	0.63	0.42	0.52	0.67	0.55	0.62	1.00										
director	0.46	0.55	0.42	0.39	0.38	0.52	0.54	0.37	0.31	0.56	0.34	0.46	0.46	1.00									
NISA	0.29	0.43	0.38	0.34	0.29	0.33	0.43	0.20	0.36	0.36	0.29	0.28	0.37	0.30	1.00								
radioactivity	0.39	0.54	0.42	0.38	0.36	0.51	0.56	0.28	0.30	0.53	0.35	0.37	0.48	0.53	0.37	1.00							
nuclear-plant	0.50	0.75	0.61	0.69	0.58	0.67	0.74	0.45	0.62	0.78	0.53	0.66	0.67	0.50	0.48	0.57	1.00						
officer	0.25	0.41	0.23	0.17	0.12	0.33	0.36	0.13	0.11	0.29	0.10	0.20	0.30	0.47	0.23	0.55	0.37	1.00					
TEPCO	0.76	0.53	0.57	0.61	0.67	0.45	0.58	0.46	0.74	0.61	0.66	0.56	0.56	0.36	0.35	0.34	0.56	0.14	1.00				
blackout	0.76	0.51	0.57	0.61	0.76	0.41	0.55	0.47	0.70	0.62	0.71	0.59	0.54	0.36	0.25	0.34	0.45	0.14	0.74	1.00			
Fukushima	0.49	0.74	0.51	0.65	0.62	0.73	0.79	0.53	0.57	0.84	0.62	0.68	0.68	0.55	0.39	0.59	0.80	0.34	0.56	0.53	1.00		
president	0.49	0.42	0.39	0.36	0.40	0.38	0.46	0.35	0.50	0.42	0.36	0.33	0.42	0.55	0.26	0.55	0.39	0.47	0.50	0.41	0.44	1.00	
vice-president	0.16	−0.07	−0.05	−0.12	−0.09	−0.03	0.02	0.00	−0.10	−0.05	0.02	−0.09	0.01	0.17	0.05	0.29	−0.08	0.31	0.06	0.02	−0.01	0.61	1.00

Fig. 7. Correlations between trigger words candidates

Twitter Bursts: Analysis of their Occurrences and Classifications

Yuhiro Mizunuma, Shuhei Yamamoto, Yutaro Yamaguchi
Atsushi Ikeuchi, Tetsuji Satoh
University of Tsukuba
Tsukuba, Japan
Email:{yuhiro, atsushi}@slis.tsukuba.ac.jp
{yamahei, yamaguchi, satoh}@ce.slis.tsukuba.ac.jp

Satoshi Shimada
Housei University
Tokyo, Japan
Email: satoshi.shimada.57@hosei.ac.jp

***Abstract*—Twitter, a microblogging service launched in October 2006, has become one of the most popular social communication media. Because Twitter's characteristics are immediacy, ease of use, and bi-directionality, its timeline reflects the real world almost instantly. Once a major event happens, the number of tweets increases rapidly. In this article, this phenomenon is defined as a burst. The authors gathered Japanese tweets on a public timeline from Twitter API over a period of fifteen months starting from November, 2011, to February, 2013. We collected over 5 billion posts created by about 11 million users. Results of our analysises show that during the bursts, the total number of tweets showed a higher percentage of retweets, fewer replies, and fewer characters used per post than those during normal status. Cluster analysis revealed five types of bursts. Furthermore, we clarified that the scale of earthquakes in Japan and the distance from the quakes' epicenters to Tokyo significantly affected the occurrence of bursts on Twitter.**

Keywords-Twitter; Burst; Clustering

I. Introduction

In our increasingly technological world, people commonly and regularly use online social networking service to connect, communicate, and obtain information. As one of the most popular social networking and microblogging tools, Twitter enables users to send and read text messages, called tweets, of up to 140 characters via computers or mobile phones. Since its launch in 2006, Twitter has rapidly increased in terms of the number of users. In December 2012, Twitter Inc. reported having more than 200 million active users creating more than 400 million tweets daily [1]. In Japan, Twitter is more popular than any other social networking tool, for instance, mixi, Facebook, Linkedln, and Google+ [2]. The number of Twitter users in Japan is the third largest in the world, after the United States and Brazil. To put this status into perspective, Japan's population in 2011 was approximately 127.8 million; Brazil 196.7 million; United States 311.6 million [3]. Twitter has been widely regarded as an effective emergency communication tool, and after the Great East Japan Earthquake in March 2011, its users increased exponentially.

Twitter's technological characteristics—bi-directionality, immediacy, and ease of use—practically ensure increase in the number of tweets during or just after an event occurs. For example, in the popular animated television film *Castle in the Sky Laputa*, the word *balse* is spoken to cast a magic spell that devastates Laputa, the film's eponymous flying castle. On August 2, 2013, as "Balse!" was spoken on the film, a high number of Japanese users simultaneously tweeted "Balse!". In fact, Twitter Inc. reported that the world record of tweets per second (TPS) was broken with 143,199 TPS. We define this phenomenon as a "burst," and this study aims to examine and classify such bursts.

We examined the burst phenomenon through quantitative analysis, with the goal of answering the following three questions: (1) Why do bursts occur? (2) What are the characteristic features of tweets in burst status? (3) How is each burst classified? To accomplish our goal, we crawled 5,285,607,227 tweets for a span of 15 months, from November 16, 2011, to February 15, 2013.

Our report of the results is organized as follows: Next section relates our research to the perspectives of similar research. Section Ⅲ describes our data crawling methodology and our burst detection method. In Section Ⅳ, we apply the results of our analysis by examining tweets' characteristic features during burst status, comparing them with tweets during normal status (Ⅳ. A). After clarifying the characteristic features, we classify each burst (Ⅳ. B). Then, we verify factors affecting the earthquake burst (Ⅳ. C). Finally, in Section Ⅴ, we summarize our findings and indicate future challenges.

II. Related Work

With such widespread use of tweeting, studies have already been conducted to clarify exactly what Twitter is and how people use it. As pioneering researchers, Java et al. [4] collected tweets on a public timeline for 2 months, from April 1 to May 30, 2007, gathering 1,348,543 tweets posted by 76,177 unique users. Through this data, they examined the users' motivations for posting and the structures of Twitter. Java et al. clarified that the diameter of the network graph based on the follow relationship was 6. They also reported that 20% of all tweets were conversational with @, and 13% contained a URL sent to share information. Krishnamurthy et al. [5] crawled not only a public timeline but also user profiles and their tweets. They collected these data using two algorithms and performed an analysis similar to that of Java et al., describing the differences between data sets. In another study, Poblete [6] collected 5,270,609,213 tweets by 4,736,629 users from 246 countries to reveal national differences in the Twitter network.

Numerous studies have examined Twitter from the viewpoint of information propagation and relationships between users. From June 6 to June 31, 2009, Kwak et al. [7] extracted 1.47 billion follow-follower relationships and 41.7 million user profiles. These researchers' results showed that 77.9% of follow-follower networks were one-way but that mutual follows accounted for only 22.1%. These features are unique to Twitter among social networking services. They suggest that Twitter's technological characteristics make it a stronger source for communicating and disseminating or obtaining information.

Many further studies of Twitter have related it to the real world. On one hand, some studies have attempted to relate tweets to later events, in other words, to predict the future through Twitter. Bollen [8] tried to predict stock prices; Asur [9] tried to predict movies' box office sales; and Tumasjan [10] tried to predict election results. On the other hand, some studies attempted to detect the actual condition of the world. From August to October 2009, Sakaki et al. [11] gathered tweet data that was used to detect earthquakes with a high probability: 96% of seismic intensity 3 earthquakes and 100% of more intense earthquakes were detected. Diao et al. [12] detected trends in event according to burst words in tweets. From September 1 to November 30, 2011, these researchers collected 3,967,927 tweets from users in Singapore. Using latent Dirichlet allocation (LDA) and two LDA improved algorithms (UserLDA, TimeLDA), they conducted automatic detection of topics from extracted words. Results showed that, using improved algorithms, their method can detect unique topics more precisely than conventional methods. Shirakihara et al. [13] obtained buzzwords from buzztter.com/. Then, using the algorithm proposed by Kleinberg, these researchers detected the time zone in which tweets including certain buzzwords increased rapidly.

In brief, most Twitter studies have focused on event detection in the real world rather than on users' information-gathering behavior and features of tweets. By focusing on the number of tweets as they increase through a certain time span, our study proposes to clarify why and how people tweet. Thus, we discuss the relationship between the real world and Twitter. In a research focused on the number of tweets, Inui [14] analyzed 179,286,297 tweets posted around the Great East Japan Earthquake that occurred on March 11, 2011, revealing that the tweets per minute (TPM) peaked in the week after the earthquake. The highest number of tweets was recorded on March 15, 2011, when the seismic intensity 6 earthquake occurred in Shizuoka Prefecture. The second highest number was recorded just after another earthquake that occurred on Sanriku coast.

III. Method

To analyze burst status, we must crawl tweet data and then set a threshold value for a burst. After detecting bursts, we analyze them. In Section III-A, we explain how we crawled tweet data and how we set the threshold value.

However, we first provide some explanation of how tweets work. To post a tweet to a particular user, one begins with "@username," and the tweet appears in the timeline of a recipient user or a user who follows both sender and recipient. This type constitutes about 40% of all tweets. The reply function, of course, makes a tweet go to a particular user-in this case, the sender of the tweet replied to. A “retweet” or a re-posting of someone else's tweet empowers a tweet receiver to spread information beyond the original tweet's followers. The retweet function is symbolized in a re-sent message by "RT@username." The rate of a retweet is a percentage of the text beginning with RT over the total number of texts; this type of retweet does not include a retweet with another user's comment, which is called the "classic retweet." Similarly, this type does not include tweets beginning with QT.

TABLE I. Data Collected

	All Data	Weekday	Weekend
The number of tweets	5,285,607,227	3,740,106,962	1,545,500,265
Average number of characters	45.76	46.15	44.81
Rate of Retweets（%）	8.82	8.94	8.60
Rate of Reply（%）	39.02	39.34	38.25

A. Data Collection

From November 16, 2011, to February 15, 2013, we collected public timeline tweets from Japan, written in Japanese, using Twitter Search API. We set the parameter language for '*ja*' (Japanese) and the geocode for a 2,000-km radius from Akashi-city, Hyogo, in order to cover only Japan. We collected 5,285,607,227 tweets posted by 10,918,410 unique users. Each tweet has its own identity (ID), the user's ID, the exact time of posting, the tweet's actual text, and so on. Table I displays fundamental statistics on the collected data. Of the 5,285,607,227 tweets harvested, 8.82% were retweets. The rate of reply was 39.02%. The mean for characters was 45.75, and the mode, the value that appears most often, for characters was 21.

B. Setting Threshold Value

For analysis of the phenomenon under consideration here, a sudden, large increase in tweets beyond the normal traffic is considered a "burst." For macroscopic analysis, of course, we must establish a quantitative burst threshold, a set value. We check the threshold every minute, and when the number of tweets rises above the threshold value, we judge that time to signal a burst. Figure 1 indicates average number of tweets according to day and time. In Figure 1, the average number of tweets at 4:00 is below 2,000 tweets par minute, and at 23:00, the average is more than 140,000 tweets par minute. This information suggested that we should not set the same threshold throughout the day, and thus, we decided to set the threshold by the minute-as Figure 1 illustrates. As indicated in Figure 1, the number of tweets also differs on weekdays and holidays. Holidays are weekends, and national holidays. On a usual weekday, Twitter traffic increases around 8 a.m. and around noon, indicating use after awakening, during the morning commute, and during lunch breaks. On holidays, however, tweeting steadily increases into the night hours. For these reasons, we set different thresholds for both the day and the time.

As Table II shows, the average number of tweets and unique users is increasing. If we applied the same threshold to all the

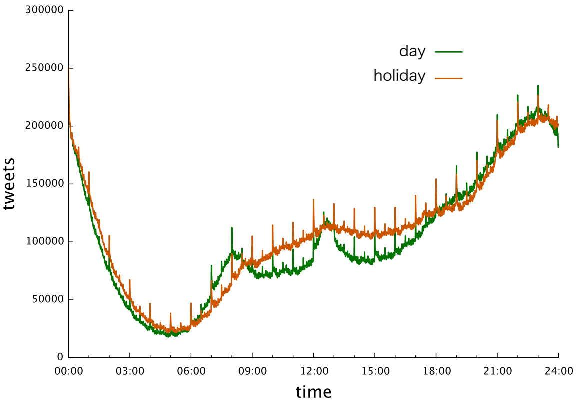


FIGURE 1. AVERAGE NUMBER OF TWEETS ACCORDING TO DAY AND TIME

TABLE II. CHANGING NUMBER OF TWEETS, USERS, AND TWEETS PER DAY

Span	Tweets	Unique Users	Tweets per User
Nov 16-Dec 15, 2011	10175500.7	113153.7	89.9
Dec 16-Jan 15, 2011	9959195.5	111298.1	89.4
Jan 16-Feb 15, 2012	10498451.5	113941.8	92.1
...	...	...	...
Nov 17-Dec 16, 2012	12302316.8	144700.2	85.0
Dec 17-Jan 16, 2013	12921195.3	145271.6	88.9
Jan 17-Feb 15, 2013	13555442.6	153905.0	88.0

data, it would be difficult to detect earlier bursts and easy to detect recent ones. Thus, we also set different thresholds for each month. To calculate the threshold value for a certain month, we used a dataset that included the month previous and the month after that under consideration. For instance, to calculate the threshold from March l6 to April 14, 2012, we used the dataset from February 14 to May 15, 2012. We detected bursts from December 16, 2011, to January 15, 2013, using data from November 16, 2011, to February 15, 2013. The threshold values for bursts were calculated using the following formula:

$$N_{nt}(t) = \overline{N}(t) + 3\sigma(t) \tag{1}$$

where $N_{nt}(t)$ represents the threshold value of a burst at a certain time(t), $\overline{N}(t)$ is average of the number of tweets per day at a certain time(t), and $\sigma(t)$ is the standard deviation at a certain time(t). For calculating the threshold value, two extreme values of tweet numbers for each time were removed from the dataset.

Based on this method, we detected 5,326 bursts from holiday dataset and 5,650 burst from weekday dataset. We detected burst events by checking tweet texts and times. Some bursts have relevance to television programs, for example, *Lupin III: The Castle of Cagliostro, Smile PreCure!,* and *Tetsuko's Room*, and bursts were caused by televised sports events as well. Justin Bieber's appearance on a Japanese television program caused a burst. In addition, a burst occurred 3 minutes after television news announced the arrest of Takahashi, the last Aum fugitive from the sarin gas attack on the Tokyo subway in 1995. All these examples suggest a strong association between bursts and television broadcasting. Moreover, bursts are relevant to other media; for example, Animation Song-Zanmai Z is a radio program that has caused bursts. In addition, Twitter has bursts unique to itself, such as "Twitter's server down!"

Furthermore, bursts have relevance to natural disasters, e.g., earthquakes, "bomb cyclones," tornadoes, heavy snow, and heavy rain. People experiencing a disaster post their situations on Twitter, and others use Twitter to disseminate information about the disaster.

IV. RESULTS AND DISCUSSION

A. *Features of Posting during Burst Status*

To clarify features of posting during bursts, we compared features of text during normal status and burst status. Table III represents the average number of characters, the rate of retweets compared to all tweets, and the rate of reply to all tweets during burst status, nonburst status, and all statuses, respectively.

TABLE III. COMPARISON OF TEXT FEATURES

	All Statuses	Burst Status	Nonburst Status
Average number of characters	45.8	42.2	45.8
Rate of retweets（%）	8.84	9.29	8.83
Rate of Reply（%）	39.02	33.83	39.15

In burst status overall, the average number of characters is fewer than that in normal status because users attempt to tweet as quickly as possible. Because time is of the essence, users make their posts short. In fact, during bursts caused by earthquakes, users posted very short texts in two or three Japanese characters, such as "Oh no!", "Earthquake," or "Shaking!" In burst status also, the retweet rates are higher than those in nonburst status, and the rate of reply in burst status is lower than that in nonburst status. Users try to spread information about burst events to many people, and thus, the retweet rates become higher. In burst status, people like to use Twitter's functions to diffuse rather than limit information. For example, during a burst on March 14, 2012, 20.9% of all tweets were retweets. On that date, an earthquake occurred, and users posted retweets of information about the disaster tweeted from a public office account: RT@zishin3255_2 Earthquake Early Warning (no.12) There was an earthquake in Sanriku offshore, 3 on the Japanese scale. [Detail] The 9.0 magnitude earthquake occurred at 18:08:29 on 14th March 2012, depth of 10 km. It will reach Tokyo at 18:11:26 [about 177 seconds later]. #EarthquakeEarlyWarning and RT@NHK_PR: There is a tsunami advisory for Iwate Prefecture and the Pacific Ocean coast in Aomori Prefecture. The Earthquake Early Warnings are issued mainly by the Japan Meteorological Agency (JMA), and NHK is Japan's national public broadcasting organization. Kwak [7] observed that Twitter is more a source of information than a social networking site, and our results confirm that, particularly during bursts, people tend to use Twitter as a source of information.

B. *Classifications of Bursts*

In the previous section, we explained that during bursts, tweets tended to be retweeted, less replies were received, and less characters than usual were contained. However, we

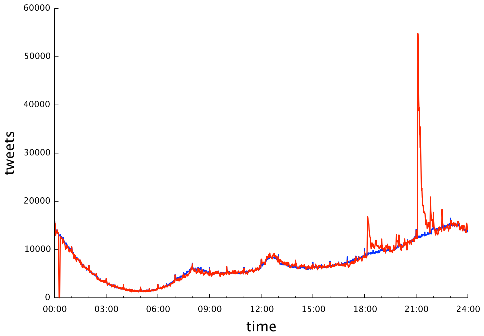


FIGURE 2. EARTHQUAKE BURST

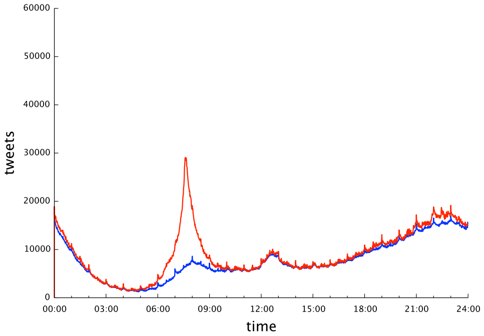


FIGURE 3. ANNULAR ECLIPSE BURST

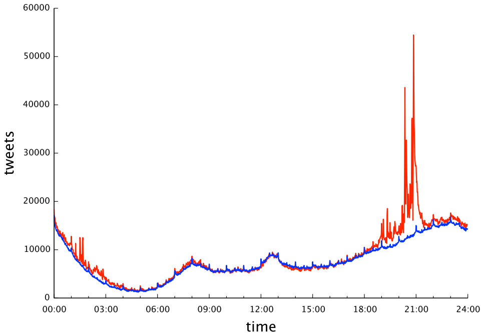


FIGURE 4. FOOTBALL (AUSTRALIA VS. JAPAN) BURST

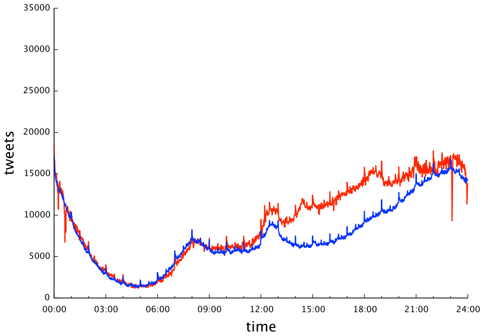


FIGURE 5. BOMB CYCLONE BURST

also framed the hypothesis that different events may cause different posting features. Hence, we tried to classify each burst according to its features, that is, the average number of characters, rates of retweets, and rates of replies. In addition, we found that the shape of a burst can indicate the type of event.

Figures 2-5 indicate the changing number of tweets according to event. For instance, Figure 2 shows the number of tweets increasing rapidly after an earthquake and then decreasing rapidly. In other words, an unpredictable event, such as an earthquake, causes an increase and then a decrease in the number of tweets within a short time span. Figure 3 illustrates the process of tweet numbers on May 21, 2012, the day an annular eclipse occurred. In this case, users knew when the eclipse would occur, and thus, the number of tweets increased and decreased moderately before and after the event. On June 12, 2012, the Fédération Internationale de Football Association (FIFA) World Cup qualifier with Japan versus Australia was played. As shown in Figure 4, a little before the game began at 19:00 and a little after the game ended at 20:50, the number of tweets was higher than usual, increasing particularly when goals were scored and when the game ended. Figure 5 illustrates tweet numbers on the day a bomb cyclone hit Japan. Different from other figures, span of increasing tweets was very long, although the distance to average was not so long. These examples, illustrated in the figures, show that Twitter users' reactions to various events can change the bursts' shapes.

We further framed the hypothesis that a burst's features reflect the event's nature. We classified the bursts and then detected the nature of events in each cluster. Each burst has data about shape, that is, (1) length of burst status and (2) distance to threshold. The *length* of burst status is the *total time between the number of tweets above and below the threshold value*. If the number of tweets goes above the threshold value at one measurement and then falls below the threshold value at the next measurement, the length of the burst is 1 min. In addition, each burst contains data regarding text features, that is, (3) average number of characters, (4) rates of retweets, and (5) rates of replies. Thus, using these five factors, we classified each burst through cluster analysis using Ward's method and the Euclidean distance of R2.15.1. Before clustering, we normalized all the data. Table IV shows the average of each feature in each cluster.

TABLE IV. RESULTS OF CLUSTER ANALYSIS

	Duration	Distance	Num Chars	Rate of RT	Rate of @
	(minute)			(%)	(%)
1st cluster	21.32	567.44	44.87	9.42	38.28
2nd cluster	549.91	4110.08	43.41	10.95	36.10
3rd cluster	54.76	1245.37	40.35	6.99	30.86
4th cluster	51.57	5366.71	31.36	5.15	20.07
5th cluster	62.40	2333.45	48.86	22.21	27.94

Of the five clusters, the first has the shortest burst status and the shortest distance to threshold. Thus, the third cluster contains small bursts caused, in this case, by a seismic intensity 1 earthquake and unexpected strong rain. Both these events affected relatively few people in a small area. The third cluster was composed of such small bursts.

The second cluster reveals the peak of a big event, with both the longest distance to threshold and greatest length of burst status. Cluster five bursts are typified by participation of many people, such as celebrating the New Year or observing the annular eclipse.

The third cluster contains bursts previous to peaking. In this cluster, the distance to threshold is longer than that in the first cluster and shorter than that in the second cluster. Similarly, the length of burst status is longer than that in the first cluster and shorter than that in the second cluster. The beginning of the annular eclipse burst, the death of Kim Jong-il, and the televised Japanese animation My Neighbor Totoro were all in the first cluster. Thus, we concluded that this cluster is a type of burst in process.

The fourth cluster has a long threshold distance, although the burst length is comparatively short. Thus, this cluster contains a type of sudden, unpredictable event, for example, Olympic game victories, a goal at the FIFA World Cup, and earthquakes.

The fifth cluster is characterized by high rates of retweeting, and thus, we define this cluster as a type of information diffusion. Along with the many retweets, the number of characters is also the greatest, presumably to provide sufficient information. In this cluster, the bursts contained, for example, the news of a phantom killer in Shibuya and the arrest of the Aum suspect Takahashi.

To sum up, we classified bursts into five types: (1) small burst, (2) burst in process, (3) peak burst, (4) sudden burst, and (5) information diffusion burst.

C. *Factors Affecting Earthquake Burst*

Twitter's nature is one of immediacy and brevity. Users can post only 140 characters, and tweets appear on the timeline as soon as the user posts. When a disaster hits, then, Twitter can transfer information more expeditiously than other media. In this section, we discuss factors affecting earthquake bursts. Clarifying the relevance between disasters and Twitter can help provide the most rapid dissemination of information about the event. Some have studied using Twitter for the immediate spread of disaster information; for instance, Sakaki et al [11] detected disaster situations using locator information and tweet texts. However, no studies have clarified the relevance between disasters and bursts.

Throughout this investigation, bursts occurred many times in disaster situations, such as typhoons, heavy rains, earthquakes, and so on. In particular, earthquakes caused burst status 106 times. Therefore, we examined factors affecting earthquake bursts, and one factor is the earthquake's scale. Most earthquake tweets are posted when the user feels the shock of the quake. The higher the quake is on the scale, the more people notice it. Besides scale, the distance between urban centers and the earthquake may be relevant to bursts since the number of tweets increases along with the population density and numbers of Twitter users in the urban centers.

In Japan, earthquakes are assigned levels on a scale from 0 to 7, with 7 being the strongest, and we used the same scale in this study. Figure 6 shows changes in the number of tweets when earthquakes are registered in the upper 5 levels on the intensity scale. The figure contains the date of each earthquake, the name of the prefecture that recorded the maximum seismic intensity, and the distance from Tokyo.

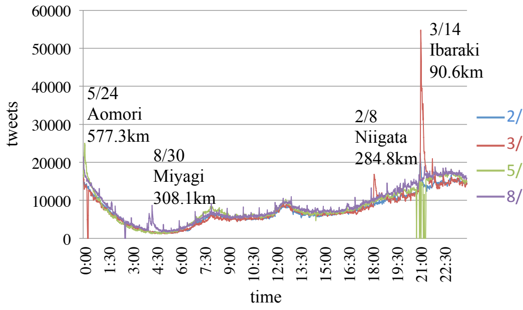


FIGURE 6. CHANGING TWEET NUMBERS IN ABOVE 5 SEISMIC INTENSITY EARTHQUAKES

This information reveals that earthquakes of the same seismic intensity do not cause the same number of tweets. The number of tweets on the March 14 is greater than that on other days. This is because of the quake's distance from the urban center. Ibaraki Prefecture is about 90 km from Tokyo, and the other prefectures are more than 100 km away. Similarly, the number of tweets after an intensity 4 quake in Aomori (May 24, 2012) was fewer than those after a less intense quake in Chiba (May 29, 2012). Now, Aomori Prefecture is about 577 km from Tokyo, but Chiba Prefecture is only about 40 km from Tokyo.

Therefore, we decided that the representative location of an urban center would be the Tokyo Metropolitan Government, with the closest seismograph station located at Kabukicho Shinjuku-ku, Tokyo. During the investigation, this seismograph station registered 50 earthquakes: 36 of intensity 1; 11 of intensity 2; and 3 of intensity 3. We detected bursts 46 times —a 92% rate of detection. These results indicate that bursts occur with high probability if the urban center experiences an earthquake.

On this basis, we adopted the hypothesis that an earthquake burst has relevance both to the scale of an earthquake and the distance from the urban center. Throughout this investigation, earthquakes of seismic intensity 3 or more occurred 341 times. We collected data for each earthquake: (1) time of occurrence, (2) epicenter, (3) maximum seismic intensity, (4) municipality recording maximum seismic intensity, and (5) distance between the urban center and the municipality. We used the earthquake database provided by the Japan Weather Association in order to collect time of occurrence, epicenter, maximum seismic intensity, and municipality that recorded maximum seismic intensity. For this study, we decided that the representative location of the urban center would be the Tokyo Metropolitan Government. The distance between the municipality and urban center was measured as the distance between the municipality's town hall and the Tokyo Metropolitan Government. We calculated the distance using Google Maps API. When more than one municipality recorded the same maximum seismic intensity, we chose the municipality closest to the Tokyo Metropolitan Government and calculated the distance. If the Twitter burst occurred within 3 min after the earthquake, we decided the earthquake caused the burst. However, if the burst occurred before the earthquake, we removed the earthquake data from our dataset. Earthquakes over seismic intensity 3 occurred 341 times. Within 3 min after earthquakes, 127 bursts occurred, but 11 of them had attained burst status before the earthquake occurred. Excluding those

11 earthquakes, we then calculated a rate of burst detection using 328 earthquakes and 106 bursts (Table V).

TABLE V. RATE OF BURST DETECTION

Distance from Urban Center	Intensity 3	Intensity 4	Above Intensity 5
Up to 100km	63.2%(24/38)	100.0%(16/16)	100.0%(5/5)
100-200km	14.0%(12/86)	57.1%(12/21)	60.0%(3/5)
200-300km	14.8%(4/27)	100.0%(3/3)	100.0%(3/3)
Over 300km	8.2%(8/98)	30.8%(8/26)	80.0%(4/5)

When the earthquakes registered seismic intensity 3, the more the proximity to the urban center, the higher was the rate of burst detection. This suggests relevance between the distance from the urban center and the burst. When earthquakes registered a seismic intensity of 5 or more, the rate of burst detection is very high, regardless of the distance from the urban center. This suggests relevance between an earthquake's scale and its resultant burst.

We performed logistic regression analysis to confirm these results. We used "burst or no burst" as the dependent variable, and "scale of the earthquake" and "inverse of distance from urban center" as independent variables. Tables VI reveal the results of logistic regression analysis using R2.15.1. McFadden's ρ is 0.26, Cox-Snell's R^2 is 0.366, and Negelkerle's R^2 is 0.488. Identification rate based on the regression equation is 80.5%.

TABLE VI. RESULTS OF LOGISTIC REGRESSION

	B	SE	Wald	p Value	Odds Ratio
Intensity	5.288161	0.703	56.657	5.2e-14**	197.98
Distance	1.354106	0.163	68.872	2e-16**	3.87

Intensity: maximum seismic intensity; Distance: Distance from urban center;
B: partial Iregression coefficient; SE: Standard error

For each independent variable, a p value less than 0.05 was considered statistically significant. The correlation coefficient between each independent variable was below 0.1. Evidence for multicollinearity was absent because the variance inflation factor for independent variables in models was less than 2.0. The results suggest that the scale of the earthquake and the distance from the urban center are affecting earthquake bursts. In particular, the value of Wald suggests that the distance from the urban center more strongly influences a burst than the scale of the earthquake.

V. CONCLUSION

This study aimed to explore the media character of Twitter by focusing on the burst phenomenon. We clarified that burst tweets are more likely to be retweets, receive less replies, and contain fewer characters than usual. In burst status, in fact, Twitter becomes more a source of information than a social site. In addition, we classified each burst and clustered burst events into groups. According to certain features, we were able to classify five types of bursts (1) small burst, (2) burst in process, (3) peak burst, (4) sudden burst, and (5) information diffusion burst. Finally, we verified factors affecting earthquake bursts, namely, that the scale of earthquakes and the distance from an urban center affect earthquake bursts, with the latter having a stronger influence than the former.

In future research, we plan to focus more on individual users. To further clarify factors affecting earthquake bursts, we should separately consider two groups of users, those who tweet after perceiving the quake themselves and those who tweet after receiving news of an earthquake. To do so, we must more finely gather geocode and time-of-posting data. We will classify users according to network and profile data and then compare burst status between the two groups. For even finer research on this data, we should detect burst events through natural language analysis.

VI. ACKNOWLEDGEMENT

This work was supported by JSPS KAKENHI Grant Number 25280110.

REFERENCES

[1] k. Wickre, "Celebrating #Twitter7". The Official Twitter Blog. 2013-03-21. https://blog.twitter.com/2013/celebrating-twitter7. (accessed 2013-08-01).

[2] Internet Media Research Institute eds. Report of social media research 2011. impressR&D, 2011, 156p. [in Japanese].

[3] Semiocast. "Twitter reaches half a billion accounts More than 140 millions in the U.S.". Semiocast. http://semiocast.com/publications/2012_07_30_Twitter_reaches_half_a_billion_accounts_140m_in_the_US. (accessed 2013-08-01).

[4] A. Java, X. Song, T. Finin, B. Tseng, "Why We Twitter: Understanding Microblogging Usage and Communities" In Procedings of the Joint 9th WEBKDD and 1st SNA-KDD Workshop 2007, 2007, pp. 56-65.

[5] B. Krishnamurthy, P. Gill, M. Arlitt, "A Few Chirps About Twitter," In Proceedings of the First Workshop on Online Social Networks, 2008, pp. 19-24.

[6] B. Poblete, R. Garcia, M. Mendoza, A. Jaimes, "Do All Birds Tweet the Same? Characterizing Twitter Around the World," In Proceedings of the 20th ACM International Conference on Information and Knowledge Management, 2011, pp. 1025-1030.

[7] H. Kwak, C, Lee, H. Park, S, Moon, "What is Twitter, A Social Network or a News Media?" In Proceedings of the 19th International Conference on World Wide Web, 2010, pp. 591-600.

[8] J. Bollen, A. Pepe, H. Mao, "Modeling public mood and emotion: Twitter sentiment and socio-economic phenomena," In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, 2011, pp.450-453.

[9] A. Asur, B. A. Huberman, "Predicting the Future With Social Media," In Proceeding WI-IAT'10 Proceedings of the 2010 IEEEWICACM International Conference on Web Intelligence and Intelligent Agent Technology, 2010, pp. 492-499.

[10] A. Tumasjan, T. O. Sprenger, P. G. Sandner, I. M. Welpe, "Predicting Elections with Twitter: What 140 Characters Reveal about Political Sentiment," Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media, 2010, pp. 178-185.

[11] S. Takeshi, O. Makoto, M. Yutaka. "Earthquake Shakes Twitter Users: Real-Time Event Detection by Social Sensors," In Proceedings of International Conference on World Wide Web, 2010, pp. 851-860.

[12] Q, Diao, J. Jiang, F. Zhu, E. P. Lim, "Finding Bursty Topics from Microblogs," In Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics, 2012, pp.536-544.

[13] S. Wataru, O. Tetsuya, H. Ryuzo, F. Hiroshi, K. Miyuki, "Report of Information Fundamentals and Access Technologies," 2010-IFAT-99(2), 2010, p. 1-8. [in Japanese].

[14] "FrontPage/Project311/trend analysis". Laboratory of Inui and Okazaki. 2012-10-13. http://www.cl.ecei.tohoku.ac.jp/index.php?Project%%E3%83%88%E3%83%AC%E3%83%B3%E3%83%89%E5%88%86%E6%9E%9. (accessed 2012-09-30).

Accessibility to Digital Society: Interaction for All

Pilar Orero, Javier Serrano, Olga Soler, Anna Matamala, Judit Castella, Maria Teresa Soto Sanfiel, Anna Vilaro, Carme Mangiron

Catalan Centre for Research in Ambient Intelligence and Accessibility, CAIAC
Autonomous University of Barcelona, UAB
Barcelona, Spain
{pilar.orero, javier.serrano, olga.soler, anna.matamala, judit.castella, mariateresa.soto, anna.vilaro,carme.mangiron}@uab.cat

Abstract— **The project HBB4ALL (Hybrid Broadband Broadcasting for All), which has just started, addresses a wide range of interactivity, interoperability and accessibility features for a multi-platform media environment – focusing on the hybrid broadcast-broadband TV (HbbTV) concept.**

Keywords: interoperability, accessibility, connectivity

I. Introduction

Since access to information was officially declared by the United Nations a Human Right in 2003, much work has been carried out by stakeholders at many levels, but still, media access deployment in Europe is not equitable. Legislation, policy and regulations have been introduced and standards were drafted to assure e-inclusion. The Commission set up a legal framework in 2007 with the "European i2010 initiative on e-Inclusion - to be part of the information society"; this called on the ICT industry to work to help disabled people access digital TV and electronic communications products. It adopted the Audiovisual Media Services Directive in 2010 [1]. However, “content” processes (from conception, production, translation, exchange and archiving to distribution and use) are still complex procedures, both technologically and commercially. All access services (be them for the elderly or for people with disabilities) are language dependent. To turn the accessibility vision into reality, the active participation of multiple stakeholders is required in the value chain. HBB4ALL will address all relevant stakeholders and all components of the value chain.

One of the prominent challenges of the coming years will be the multi-platform delivery of audio-visual content (anytime, anywhere, any device) [2], be it a broadcast or a (future) Internet (IP) TV service. Hybrid delivery platforms such as connected TVs and two-screen solutions will be ubiquitous. One aim is to automate, to the extent possible, the production of access services. Subtitling accounts for 0.2-0.5% of production budgets in large countries and up to 1% in small countries. While subtitles do not demand large data-rates for their transmission or retrieval audio description (AD) and audio subtitles (inter-lingual subtitles) are more cost-incentive and require somewhat higher data rates. Offering visual signing is most demanding in terms of bandwidth and production costs whilst - on the other hand- the target audience is relatively small. So, the other aim must be to balance the provision of access services to audio visual content between broadcast delivery (satellite, cable and terrestrial networks) and Internet (IP) delivery. At the same time, care has to be taken of new technological possibilities offering new or improved access services for the end user. Everyone who needs a specific service should be able to use it and, to the extent possible, and customize it to his or her personal needs.

The HBB4ALL project builds on HbbTV, as the major European standard, for converged services and looks at both the production and service sides. HbbTV 1.x devices are widely available in the market while HbbTV version 2.0 is currently under development. HbbTV provides a straight-forward specification on how to combine broadcast and broadband content plus interactive applications. TV content can be enhanced with additional synchronised services in a personalised manner. For access services this opens an entirely new opportunity for users who may choose an access service delivered via their IP connection which then seamlessly integrates with the regular broadcast programme.

The project will identify improvements to existing access services and ways of addressing the key technical, organisational and legal obstacles to the sustainable take-up of these services throughout Europe. Both quality and quantity metrics will be addressed in a user-centric approach. The project will offer new insights from the fields of human machine interaction and social innovation, given the fact that a new interactive multimodal and multilanguage service will be offered. This paper will first describe the structure chosen for the project, with four pilots developed in parallel. Then, it will describe the methodology and research approaches for the tests regarding quality benchmarking and measurements.

II. Methodology

The project is divided in four pilots. They will take place in a synchronic way, in the 36 months during the life of the project. Pilot 1 deals with Multi-Platform Subtitle Services. Across Europe, broadcasters are working to provide subtitles on multiple platforms for individuals who are deaf and hard-of-hearing, or do not have sufficient language skills to understand the content without textual support either in the original or foreign languages. The main challenge is to provide subtitles tailored to the specific needs of the end-users in terms of channels, platforms and consumption requirements. This requires a well-conceived production and distribution strategy that allows for the exchange of subtitles and their automatic re-purposing producing quality and impact-driven access services for multiple platforms. This pilot is a thematically clustered and cross-country, and is driven by three major factors:

- In a converged world there is a demand for distributing subtitles through additional output channels while economic pressure prevails.
- New technological options, fostered by the market penetration of IP-based services and of HbbTV as successful open standard for Connected and Hybrid TVs – allowing for improved individual rendering of subtitles through customisation by the user.
- Technology has matured to allow for automated generation of subtitles which benefits broadcasters through cost reduction and productivity increase and viewers through an increase of subtitled programmes on offer.

One of the new channels to be served by subtitles are VoD (Video on Demand), services which have become increasingly popular, given the growing penetration of HbbTV which has led to a multitude of catch up TV portals throughout Europe. Using the example of HbbTV such a service is technologically possible but simply not available up to now on connected TVs. For the current (2013) generation (version 1.*) of HbbTV-enabled devices there is no standardised implementation of features for a synchronisation of video with other data streams. Here, service providers need to implement JavaScript mechanisms requiring considerable processing power in the TV-device. Ultimately, this might lead to interoperability problems. The worst case scenario is that it would influence overall device behaviour. In HBB4ALL new and updated mechanisms for synchronising video and subtitles within an HbbTV-based player will be analysed and chosen for integration.

A new trend is the automatic multilingual generation of subtitles. Real-time subtitling through automatic speech recognition and subtitle machine translation into other languages is starting to be employed to support professional multilingual subtitling and increase its productivity. Although the quality of the automatically generated subtitles is still far from professional without manual post-edition, subtitling automation functionalities could be very useful and desirable in a wide range of applications within the HbbTV paradigm. This pilot will make available advanced HbbTV automatic multilingual subtitling functionalities, building up on technology currently under development in the European SME-DCL SAVAS [3] and CIP-PSP SUMAT [4] projects. Its application will be tested in a newsroom use-case scenario where the feasibility of automatically generating multilingual subtitles of real-time news relevant at international level.

Pilot 2 deals with alternative audio production and distribution. Given EU citizen mobility, TV content is not only seen by nationals, but also by large communities living away from home. There is also a need to broadcast same content in different languages synchronically (e.g., Swiss TV or Brussels TV) but the content is not the same across languages. Hence, having different languages for one programme is one of the major aims of the project. DVB (Digital Video Broadcasting) has the technical requirements for playing different audio tracks synchronised with one broadcast video. This is being done already e.g. for additional audio description or dual-language provision at ARTE TV channel or the Catalan TV3.

Since the upcoming specification of HbbTV 2.0 will offer a solution for synchronized IP and DVB reception, additional audio tracks can be also transmitted via IP to save bandwidth in the broadcast channel. This feature offers several possibilities within the scope of HBB4ALL. Transmitting additional language streams with HbbTV 2.0 is one of the testing opportunities this pilot is aiming. Especially for hearing-impaired people the dialog intelligibility of TV audio signals is a key criterion. Due to various reasons, the intelligibility of current TV audio mixes is often assessed as insufficient by users, including elderly, non-native speakers as well as hearing-impaired people. Investigations of the UN show a continuous increasing average age in Europe for the next decades [5], so the percentage of hearing-impaired people will consequently also increase. Hence, another major objective of this pilot is to enhance the dialogue intelligibility, as it would be beneficial for these groups. HBB4ALL will offer users the possibility to adjust the dialogue intelligibility to personal preference and will transmit clean audio enhanced streams by exploiting HbbTV 2.0 features. For Web-only TV services such as VoD, more sophisticated personalised solutions will be demonstrated since modern browsers offer the full set of HTML5 functionalities. A third group benefiting from this pilot is people with vision disabilities. A common practice is to support these groups broadcasting an extra audio channel using DVB-T (Digital Video Broadcasting Terrestrial) facilities. The AD channel contains a description of the action mixed with the dialogue. This technique allows vision impaired users to follow what is going on in a far more effective way than by hearing the dialogue alone.

Pilot 3 looks at automatic User Interaction (UI) adaptation and smart TV applications. During the last years digital TV as a media platform has increasingly turned from a simple receiver and presenter of broadcast signals to an interactive and personalised media terminal with access to traditional broadcast as well as web-based services. Actual TVs (Connected TV, Smart TV) already turn the TV into an application platform and service terminal. At the same time it is recognised that some user groups like elderly people with different kind of impairments still face problems when using those services. Approximately half of the elderly people over 55 suffer from some kind of functional limitations (vision, hearing, motor and/or cognitive). For these users, interaction, especially with PCs or other consumer electronics devices, is sometimes challenging. Often people have problems to connect their TV to the Internet, not to mention the barriers raised by digital menus and EPGs (Electronic Programme Guide). However, accessible ICT applications, e.g for social media, education, health monitoring, telemedicine, etc., could make a difference for their living quality. They have the potential to enable or simplify participation and inclusion in their surrounding private and professional communities. The Digital TV industry is following different approaches for the deployment of such services. On one hand, there is HbbTV as a standardised application platform, which provides means to host broadcast channel oriented content and application services. On the other hand, most Smart TV manufacturers maintain their own proprietary application environments (e.g. app stores, middleware) on the device, as it is the case for Google Android or SAMSUNG's Connected TV. These environments are often available in addition to broadcast and HbbTV services. Service providers that aim to target the elderly society using those application platforms would benefit largely from a solution that enables accessibility for such services. However, the availability of accessible or customised user interfaces, being capable to adapt to the specific needs and requirements of users with individual impairments is nowadays still very limited. There are numerous APIs available for various operating systems or application platforms (e.g. in Web browsers) that allow developers to provide accessibility features within their applications. Further there are of course many assistive devices and technologies available, especially for people with specific impairments (e.g. brail code rendering, screen readers, eye tracking, etc.). The key issue is that none of them offers features for automatic adaptation (and personalisation) of user interfaces. Moreover, the provision of accessible user interfaces is still expensive and risky for application developers, as they need special experience and effort for user tests. Many implementations simply neglect the needs of elderly people locking out a large portion of their potential users. The aim of this third pilot is to provide a web-based service that would allow the personalisation and adaptation of user interfaces for Connected TV services running on HbbTV 2.0 based platforms. The accessibility features of such a service will make use of the UI adaptation framework that was developed within the European project GUIDE (Gentle user interfaces for elderly people) [6]. GUIDE provides an open source software framework as well as design tools that support Smart TV service providers in efficiently integrating accessibility and personalisation features into their services considering especially the needs of elderly users with mild impairments, with features for HTML5 such as the adaptation of font sizes and colour schemes. The targeted web-service will include functions for user management and profiling, a standard application that allows user testing and profile initialisation based on different accessibility tests as well as a UI adaptation service that gives feedback and recommendations to the SmartTV application how to adapt the UI rendering according to the need of the individual user. Service providers will be capable to easily include those UI adaptation features into their services using the API of the GUIDE framework.

The last pilot is that related to sign language translation. Visual signing for audio visual media such as film and television was shown for the first time in 1929 as a means to make such content accessible to individuals whose mother tongue is a sign language and not an oral language. Users of sign language are often born deaf. In many European countries, there are constitutional and legal provisions to assure the provision of sign language for such citizens who, in numerical terms, account for less than 1% of the population.

Over the last 3 decades, broadcasters have moved from a single platform (analogue terrestrial broadcasting) to multi-platform digital distribution. Signing on analogue TV has traditionally been an open service, with the sign language interpreter being located either in a small window at the bottom of the screen or on the right-hand side of a the screen, as shown in the photos in Figures 1 and 2.

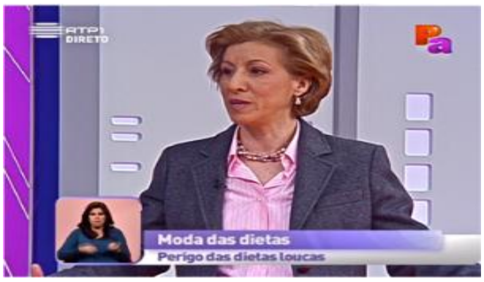


Fig 1. Signing on RTP1, Portugal

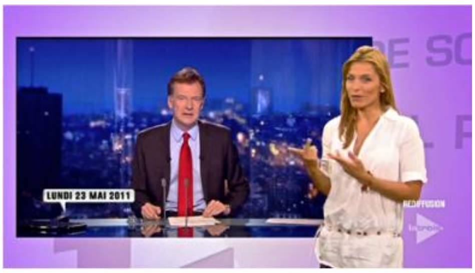


Fig 2. Signing on RTBF, Belgium

User studies reported in the EU project DTV4ALL document [7] that the RTP solution (fig. 1) with the interpreter in a small window is not optimal, as the picture-in-picture does not contain enough detail. Viewers of sign language prefer solutions like the one used by RTBF (fig. 2) and many other broadcasters. Existing television audience research suggests that, with the noticeable exception of television in Portugal (where RTP has more than 4,000 hours of signing annually, also in prime-time), viewers who do not use sign language interpreting on TV often object to 'open signing' (the inclusion of a sign language interpreter in the television picture for all viewers). While it is possible to offer a second channel, or a second video stream, with signing in the digital broadcast either as a fully-formatted video signal or as a 'widget' overlay, these are expensive as it requires additional transmission bandwidth –a least 2 megabit/second. Internet or integrated broadcasting (to the main TV screen or to a Second Screen) are thus cost-effective delivery options for closed signing (optional) services. For example, Sweden's TV4 has been delivering sign language interpretation via the internet since late 2011. On modern TV sets that also have an Internet browser, viewers can select this option on their TV sets. German public service broadcasters have been looking to use HbbTV as a delivery mechanism for sign language interpretation. In the first instance, a fully-formatted channel including the interpreter can be delivered via the Internet. The current release of HbbTV already supports this option, which would rarely call for more than 2-3,000 simultaneous streams in a given area covered by the broadcast signal. In the medium to long term, the aim is to use HbbTV 2.0 (which contains a good synchronization mechanism) to handle the presentation of a widget that is overlaid on top of the existing broadcast signal delivered via DVB, if the terminal hardware is supporting the parallel decoding of two video streams. There are correlations to captioning/subtitling, in that the HbbTV option would allow for a greater degree of viewer customization (determining the size and position of the interpreter on the screen).

Broadcasters dependent on advertising express concerns that an obligation to offer signing would lead to a noticeable reduction in advertising revenue, since audiences dislike screen contamination with the interpreter. Offering closed signing (where the viewer can choose to see or not to see the interpreter) requires much more bandwidth than closed subtitles or audio description. Signing is important not only for mainstream programming and TV programming specifically for the signing communities in Europe and elsewhere but also emergency alerts on TV. Citizens need to be informed of risks of natural or man-made emergencies and told what action they should take. This issue is underscored in the forthcoming guidelines for signatories of the UN Convention on the Rights of Persons with Disabilities that specifically mentions metrics for television targeting deaf communities.

Discussions on the Digital Dividend (the use to which radio frequency spectrum could be put following the transition from analogue transmission to more efficient, digital technologies) have not lead to bandwidth allocations in digital terrestrial broadcasting earmarked for signing. A solution to this challenge is becoming urgent, as the regulatory pressure to offer signing increases while bandwidth in broadcast networks becomes ever more costly.

III. EXPECTED RESULTS

Being an ETSI standard, HbbTV is currently linked with the DVB TV system family but can, in principle, be used in conjunction with any digital TV service in the world. DVB is widely used throughout all continents. Sooner or later, all countries in the world will have completed their analogue-to-digital switch-over. As a consequence, the results of HBB4ALL will be of worldwide relevance and will, through standardisation bodies such as the ITU and ISO, also be publicised on a world-wide level. Given the impact in close fields such as eHealth and eEducation, for example, the results from this project will have important results and direct impact. On its basis, HBB4ALL is elaborating pertinent guidelines, guides of good practice, metrics, and recommendations and will initiate campaigns to promote the project results, and thus raise awareness not only on the necessity of access and interaction services but also on the technical solutions available with interoperability. For that purpose, all relevant stakeholders, from content providers to user associations, will be addressed.

IV. CONCLUSION

The overall objective of HBB4ALL is to become a major platform/player in the e-Inclusion economy currently taking place, fostering the future market take-up of exiting innovations in conceiving universal accessibility tools and concepts to satisfy the diverse interests of all societal groups.

ACKNOWLEDGMENT

The HBB4ALL project is being developed by the Centre d'Accessibilitat i Intel·ligència Ambiental de Catalunya (CAIAC), at UAB, and it has been partially funded by FP7 CIP-ICT-PSP.2013.5.1 # 621014

REFERENCES

[1] http://ec.europa.eu/avpolicy/reg/index_en.htm

[2] NEM Position Paper on Connected TV, December 2012 http://www.neminitiative.org/fileadmin/documents/PositionPapers/NEM-PP-015.pdf [retrieved 16.11.2013]

[3] http://www.sumat-project.eu/ [retrieved 16.11.2013]

[4] http://www.fp7-savas.eu/ [retrieved 16.11.2013]

[5] United Nations – Department of Economic and Social Affairs, Population Division (2011). World Population Prospects: The 2010 Revision.

[6] http://www.guide-project.eu/ [retrieved 16.11.2013]

[7] http://www.psp-dtv4all.org/ [retrieved 16.11.2013]

On the Utilization of Smart Gadgets for Energy Aware Sensitive Behavior

Gerold Hoelzl, Peter Halbmayer, Harald Rogner, Chen Xue, Alois Ferscha
Institute for Pervasive Computing
Johannes Kepler University Linz
Austria
surname@pervasive.jku.at

***Abstract*—The conscious, efficient, and economical consumption of energy is being identified recently as crucial topic for industry, politics, and research. Limited earth resources that are still used for the majority of energy production head towards increasing energy prices and stress world climate and the budget of people. We present the PowerIT System that utilizes smart gadgets to achieve a more efficient and economical use of the available energy. By providing instant feedback of the current energy consumption in households by leveraging power metering technology and therefore raising awareness about the economics of the own energy usage, this work aims at reducing the energy consumption of people in their homes. The real-time energy consumption is captured, whereas the power signatures of electrical devices measured by power metering systems are the input modality for the system. This data is provided in real time as visual feedback to the residents using today's available smart gadgets (e.g., smart phones, tablets, and smart watches) in order to raise awareness about the current power demands. Beside the pure monitoring and control of power consumers, the system additionally collects data about the activities of people by using smart watches. This data can be used to generate activity models resulting in activity aware power saving schemes. We argue that the awareness of people about their energy consumption can induce a behavioral change resulting in a more efficient use of energy without affecting their level of living.**

Keywords*—*Power Management; Efficient Power Usage and Power Awareness; Behavioral Change; Sensor Networks; Activity and Context Recognition; Smart Gadgets.

I. Introduction and Motivation

It should be common knowledge that energy is a scarce resource. In opposite to that knowledge, we see a dramatic increase in the use of energy in the last years [1]. Due to the fact that our society is not aware of how many energy they consume, a technique of unobtrusively making them aware of their daily energy consumption should be identified. We focus on electrical energy as a part of the global energy composition because its consumption can be controlled and changed easily by people. Hoelzl showed in [2] that with the utilization of context [3] data in households, in this case the modes of locomotion in combination with different locations, it was possible to save on average 17% of electrical power. As the results were mostly gained by analyzing a collected dataset of 15 households, we focus in this work on deploying a realtime system to bring the gathered results out in the field.

The last years, especially the last months showed that the developments in the consumer market proved the augur that everyone would be able to get a wearable digital and smart artifact. Concerning nowadays developments, these gadgets are becoming smaller and smaller and people tend to use them as artifacts of daily living. Starting with the development of *smart phones* [4] that is de facto standard equipment of people in the researched living habits, the development goes towards 24 hours usage of smart watches [5]. We argue to make use of these already deployed gadgets to make users aware of the current electrical power consumption of their household devices and to control them in an unobtrusive way. As the definition of unobtrusive is recognized differently by different people, a value sensitive design [6] has to be taken into consideration when designing such a system. We made our system working completely autonomous without the need of any user interaction. It's incumbent upon the user if interaction with the system is wanted on different levels (be referred to Section III for further detail).

Using our system, the user is aware, at each point in time, of his energy consumption in realtime for each connected single device. This is a tremendous benefit compared to the nowadays deployed SmartMeter Technology were the data has a resolution of up to 15 minutes, is only available with one full day lag due to legal aspects (depending on the used technology and countries, here exemplarily picked for Austria), and can only be viewed for the aggregated power consumption of all the devices in the household. Concerning the facts that, (i) the measurements are not available for single devices, (ii) have a big lag in time, and (iii) that the measurements can be transmitted or stored at third party entities (e.g., energy provider) one is not in control of, raising security and privacy issues [7], [8] of people that they are spied on, we designed the system to capture energy readings at an interval of 10 seconds for each single energy consumer. This data is kept completely local as the system can operate without any Internet connection. Only if the user agrees on it, the data can be transmitted to a remotely connected storage.

To alter or at least to influence the behavior [9] of people is an ambitious goal that can not be fulfilled immediately. It is more or less a long term process, or to be more precise, an evolution. Fogg describes in [10] that three elements must converge at the same time to affect behavioral change: (i) Motivation, (ii) Ability, and (iii) Trigger. From our point of view the motivation of people is high, because saving energy directly affects their budget in a positive way. The missing thing is a tool, to give them an easy way to observe and control their power usage. We developed a system that can be split into two distinguishable components: (i) a completely autonomous system that records and analyzes the power consumption of connected power consumers (as described in Section II) and (ii) an easy to use App based on the Android Framework that can be installed on already deployed smart phones or tablets to monitor and control the electrical power consumptions in an unobtrusive way (see Section III). Using this App, people become aware of how many power their electrical devices consume when they are turned on, or when they are in standby mode and can react accordingly in, e.g., turning them completely off using the App to avoid standby losses.

Beside the pure monitoring and control capabilities, the use of sensory input that can be used to infer user activities, thus can be used for implicit control of energy consumers, is the last major aspect of the system. Recent advancements in Activity Recognition [11] deal with long-term evaluations to achieve higher performances and better recognition rates. Todays available results are mostly gathered in closed and controlled laboratory settings [12], [13]. Bringing this research out in the field, to collect real world data for empirically underpinning the research results with a highly flexible system, as sensors can dynamically appear and disappear [14], [15], [16], on a large scale can improve the recognition models dramatically [17].

The remaining paper is structured as follows. Section II describes the System Architecture that is used for autonomous collecting energy consumption and user activity data. In Section III we present the interaction gadgets that can be used to monitor the system and keep the user up to date about the energy consumption in realtime. The deployed hardware components of the system and the first preliminary results gathered during the first rollout phase are described in Section IV. Section V closes the paper and summarises the achievements.

II. System Architecture

To measure and collect the energy consumption of power consumers, to control them, and to record the user activity data via a wrist worn smart-watch sensor platform, we defined the architecture of the PowerIT Framework as shown in Figure 1. For each power consumer that is connected to the system, an *Energy Consumer Control* device has to be plugged between the device itself and the power outlet. Using the Energy Consumer Control Unit, the system is capable of monitoring the power consumption and to switch the connected device on or off. Using a power distribution block, it is possible to form ensembles of devices (e.g., home entertainment system consisting of the smart TV, surround sound, and the video recorder) that are treated as one 'single' device. The Energy Consumer Control unit is connected, dependent on the household infrastructure, via WiFi or Power-Lan-Communication (PLC) [18] to the Background Intelligence. PLC utilizes the already exiting electrical wiring infrastructure in households for networking and communication thus eliminating the expense and inconvenience installation of new wires or antennas.

The Background Intelligence is responsible for managing the Power Readings from the Energy Consumer Control Units. This includes the storing of the data, its synchronization, its realtime analyzation (device in on-, off-, or standby-mode) and its preprocessing for visualization in the PowerIT-App. Beside the management of the collected power readings from the different devices, the Background Intelligence also handles the collection of the Smart-Watch activity readings. This consists of storing the raw accelerometer readings and the corresponding User Activity (i.e. the semantic label that marks the activity of the user). Capturing this sensor data via an easy to use smart-watch allows to build a comprehensive dataset in a real world setting. Having the activity labels of the users allows to relate the used power consumers to the activities of the user. If this relation is known, one can implicit control power consumers in turning them on or off according to the current activities of users.

Beside the pure collection of generated power consumption and user activity data, the Background Intelligence also manages the User Generated Control Messages. These Control Messages allow users to explicitly switch power consumers on and off. Based on an Energy Management Constraint Set, that contains conditions that always have to be met (e.g., never turn the fridge off), the User Generated Control Messages are forwarded to the Power Consumer Control Logic that is responsible for transmitting the message over the network (WiFi, PLC) to the corresponding Energy Control Unit.

Location Information [2] is seen as an important part of context data. Accurate Indoor Positioning is still an open issue always connected with high costs and maintenance effort (e.g., body worn sensor equipment, learning of RSSI or WiFi Maps, etc.). Nevertheless it can contain useful information for an energy management system that can react according the location of persons in the household (e.g., all people are in the living room can imply to turn off the lights in all other rooms). In the proposed architecture, this information is (i) transmitted directly from a user worn location / positioning sensor, (ii) inferred from the Power and Smart Watch activity readings or (iii) used to cross-validate (i) with (ii) and vice versa. Deploying the proposed architecture out in the field will show which resolution of location data is necessary and useful for an energy management system. This can range from cartesian coordinates to a spatial abstraction at room level.

To enable the proposed system to work completely autonomous, in turning power consumers on and off implicitly without any needed interaction from the users, an Energy Management Rule set can be defined. Based on the Event-Condition-Action principle, each rule consists of the tuple <Person, Activity, Location, Time/Date> and triggers a defined set of *Actions* in terms of turning power consumers on or off. Based on the Power Readings, the Smart-Watch Activity Readings, the Location Information, and the Time&Date, the system can autonomously switch to predefined energy management states. This system behavior needs, on the one hand nearly 100% accurate sensor data and on the other hand a well defined rule set that has to be defined for each household. Neither of them is easy to achieve. In many complex houses the level of granularity can require some aggregation. Evaluation of the system over time will show the level of granularity at which implicit, rule based power management is possible and brings benefit to the users.

In this section, we described the system architecture of the PowerIT-System. It consists of two parallel working principles, specifically (i) an autonomous data collecting unit for Power and Activity Readings, and (ii) and explicit control and monitoring unit were the user can switch electrical power

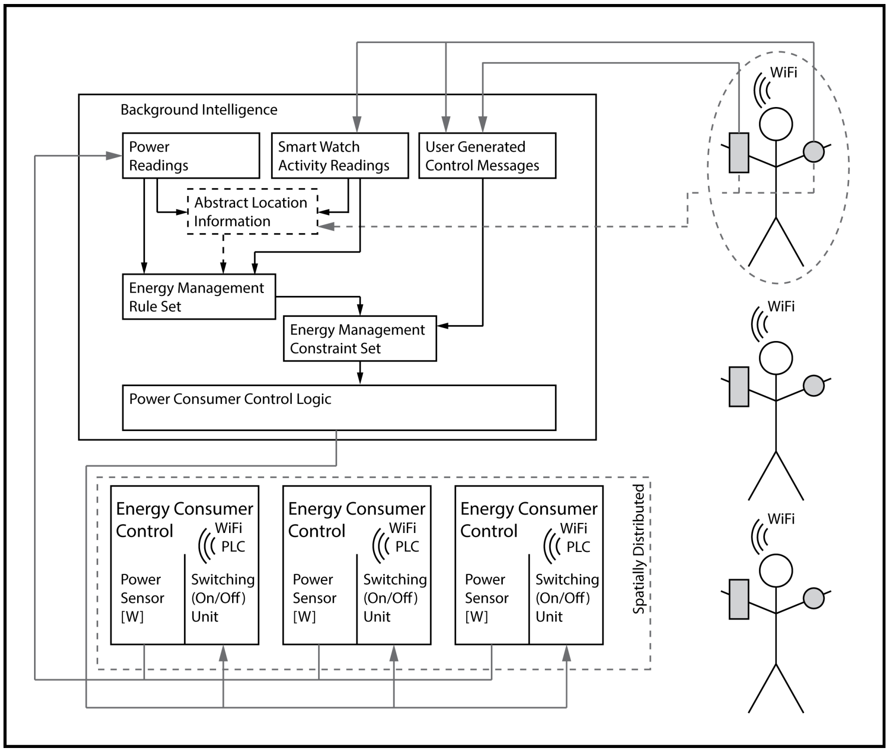


Fig. 1. System Architecture of the deployed Smart Energy Management System showing its components and their interplay as described in Section II.

consumers on and off. Switching a device off means completely disconnecting it from the power supply and therefore zero power consumption. Having the ability to autonomously collect power and activity data allows, on the one hand to generate power statistics and profiles over time (e.g., aggregated power usage of the monitored devices (be referred to Section III)) that can be shown to the users to make them aware and sensitive to their power consumption, and on the other hand to collect data sets and time use surveys to train accurate activity models. If the activity models are accurate enough, the proposed system could work completely autonomous and adjust the power consumption using the Energy Management RuleSet (i.e., the used electrical devices) accurately to the needs of the users.

III. User Experience and Awareness

The PowerIT system (as presented in Section II) is designed to collect and analyze data in an completely autonomous manner once deployed. As the user should be made aware of his energy consumption, we developed a PowerIT App that can be used by the user on variant different gadgets (tablet, smartphone, and smart-watch) to monitor and control the system at various levels. The user involvement is different at each of the 4 levels. It raises from level 1 to level 4 and is explained in detail below:

1) *Energy Consumption Recognition and generating of Load Profiles for each connected device.*
This is done completely autonomously by the system for each connected power consumers. Results can be shown in real-time for the current energy consumption and for informative purposes for all collected data on a daily, weekly, monthly, and yearly base.

2) *Collection of raw sensor data from the Wrist Worn Sensor (3-axis accelerometer) of the Smart Watch sensor platform.*
In principle, this process is also handled by the system in a completely autonomous manner. The involvement of the user is limited to wearing the smart-watch.

3) *Assignment of User Activity Metadata to the recorded sensor data via the Smart Watch (exemplarily shown in Figure 2; The Activities from left to right are: Travel, Eat, Education, Entertainment, and Family-Care).* Users can select a subset out of a set of 28 predefined activities that best fit their needs and makes selection more easily. Additionally the set can be extended by user defined activities for flexibility reasons.
The user has to set the current performed activity by selecting the correct activity label on the smart watch. Dependent on the granularity of activities, the user involvement can be quite high.

4) *Implicit power consumer control based on a user defined Energy Management Rule Set and the collected sensory data that is used as input for the system.*
This implies (i) a fully trained activity recognition model and (ii) a defined rule set which power consumers are activated based on the sensory input. This level needs high user involvement in training the activity model where steps 1-3 build the base, and in defining the energy management rule set. Especially when more than one person lives in a household, resolving conflicting rules can make the rule base unmanageable. This is especially true when the rule base management is done by non experts.

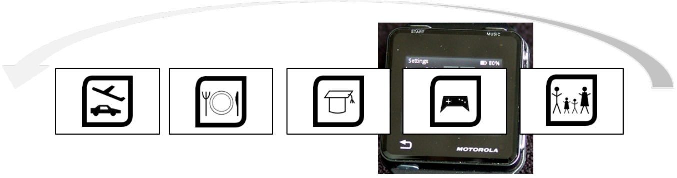


Fig. 2. Realtime assignment of the User Activity to the collected Sensor-Data on the wrist worn Smart Watch Sensor Platform.

Beside the above presented four levels of user involvement, the user is, at each point in time able to monitor and control the system using the PowerIT-App (as shown in Figure 3) that can be deployed on android based tablets, smartphones, and smart-watches. The center of the app is a floorplan containing all attached electrical power consumers (as shown in Figures 3.ii and 3.iii). This novel navigation schema allows the user to swipe through his home in a natural way. For each room, the corresponding devices are displayed (presented in Figure 3.iii). The user can select one of the shown devices to see the current, real-time energy consumption and an zoomable energy consumption history log for the one device (see Figure 3.iv). This makes the user aware about how many energy the electrical equipment in the household is consuming. This is especially interesting for the so called standby modes, where power consumers are expected to consume power near the 0 watt level that is usually not the case. This, without the PowerIT-App, often unperceived waste of energy can be prevented. Therefore, the PowerIT-App offers the possibility to fully disconnect the power consumer from the power supply in simply switching it off (as long as it is not prohibited by the Energy Management Constraint set as described in Section II). The on/off switch is placed in the device view so the user gets a realtime feedback that the device is now consuming 0 watts as it is completely disconnected from the power supply by the Energy Consumer Control Unit (see Section II).

In this section, we briefly discussed the smart gadgets that can be used by people to interact with the system. The focus was to build on the one hand an easy to use phone- or tablet based App that makes the user aware of his power consumption and on the other hand a smart-watch based App that allows to record and annotate user activities in an easy and unobtrusive way. The interface design of the App allows easy navigation through the household based on a floorplan. Electrical devices can be selected, their realtime power consumption can be viewed, a zoomable power-history is available, and they can be switched on or off. Furthermore, the power consumption can be aggregated for free definable time spans (preset: current day, week, month, and year) at device, room, floor, and building level. Using these options people get aware of how many power their devices are using and when. Having this information at different levels of granularity, they may tend to alter their behavior to a more efficient use of energy if they want.

In addition to the phone- or tablet based PowerIT App we ported its functionality also to a smart-watch. Extending the above described functionality, the smart watch allows to record activity data, in this case the raw values of a 3-axis accelerometer, that can be annotated with the corresponding activity by the user (as exemplarily shown in Figure 2). Depending on the quality of the annotated data, that consists of the energy consumption of the monitored devices and in addition the raw values of a 3-axis accelerometer of the used smart watches, activity models can be trained to implicitly control the system in the future. If it is sufficient to just take the smart watch to infer the user activities, as human behaviour and activity has a high variance, will be analyzed offline using the collected dataset.

IV. Deployment and Preliminary Results

To deploy the systems in households and test its suitability for everyday use, we defined a Deployment Kit Case consisting of four MotoACTV Smart Watches (Figure 4.i), one Low Power Embedded Computing Platform (PandaBoard) that hosts the Background Intelligence (described in Section II), and twenty Energy Consumer Control Units. The technical description of the deployed hardware components is presented in Table I. The PowerIT-App (as described in Section III) was deployed on the tablets and smart phones of the test household residents if available, otherwise we gave them a Nexus 7 with the preinstalled App. We are currently testing the system in two households with 3 (man, woman, son) and 4 (man, woman, son, daughter) people in parallel. After the test period that will last up to 4 month, and depending on the gathered results, we plan to deploy the system in up to 20 households to get representative data on a larger scale.

The needed deployment and setup steps for the system once arrived at a household are described in the following:

1) Unpack Deployment Kit Case and Check for completeness of Components.
2) Setup Background Intelligence System (PandaBoard)
3) Create the Floorplan (Rooms and assigned devices) of the Household using the Web-Service of the Background Intelligence.
4) Deploy Energy Consumer Controls according to the created Floorplan and Devices and check their communication (PLC, WiFi) network.
5) Deployment of the Smart Watches to the household residents.
6) Register Metadata (Person,- and Device Information) using the Web-Service of the Background Intelligence.
7) Initial test of all system components (Energy Consumer Controls, Background Intelligence Platform, Wrist Worn Smart Watch, PowerIT-App).
8) Introduction of the system usage to household residents.

TABLE I. TECHNICAL DETAILS OF THE DEPLOYED HARDWARE COMPONENTS OF THE SYSTEM.

MotoACTV: Processor: ARM Cortex-A8; Frequency: 600Mhz; Memory: 256MB RAM, 8GB Flash; Radio: 802.11b/g/n, BT 4.0, Display: 1.6” 220x176 capacitive multitouch LCD; Sensors: GPS, Accelerometer, Ambient Light, Compass; Weight: 35g; presented in Figure 4.i.
PandaBoard: Processor: ARM Cortex-A9 MPCore; Frequency: 1.2Ghz; Memory: 1GB RAM; Weight: 74g; presented in Figure 4.ii.
Energy Consumer Control Unit: Processor: ARM Cortex-M3; Memory: 256KB Flash Memory, 96 KB SRAM; Interfaces: UART, SSI, I2C, I2S, CAN, Ethernet MAC and PHY, USB; presented in Figure 4.iii.

To clarify the usage of the different system components, Figure 5 shows the schematic of the components used in the demonstration setup as shown in Figure 4.iv. to test the system for longtime stability. Four devices, a Coffee-Machine, a Radio, a Lamp, and a TV are connected to the system

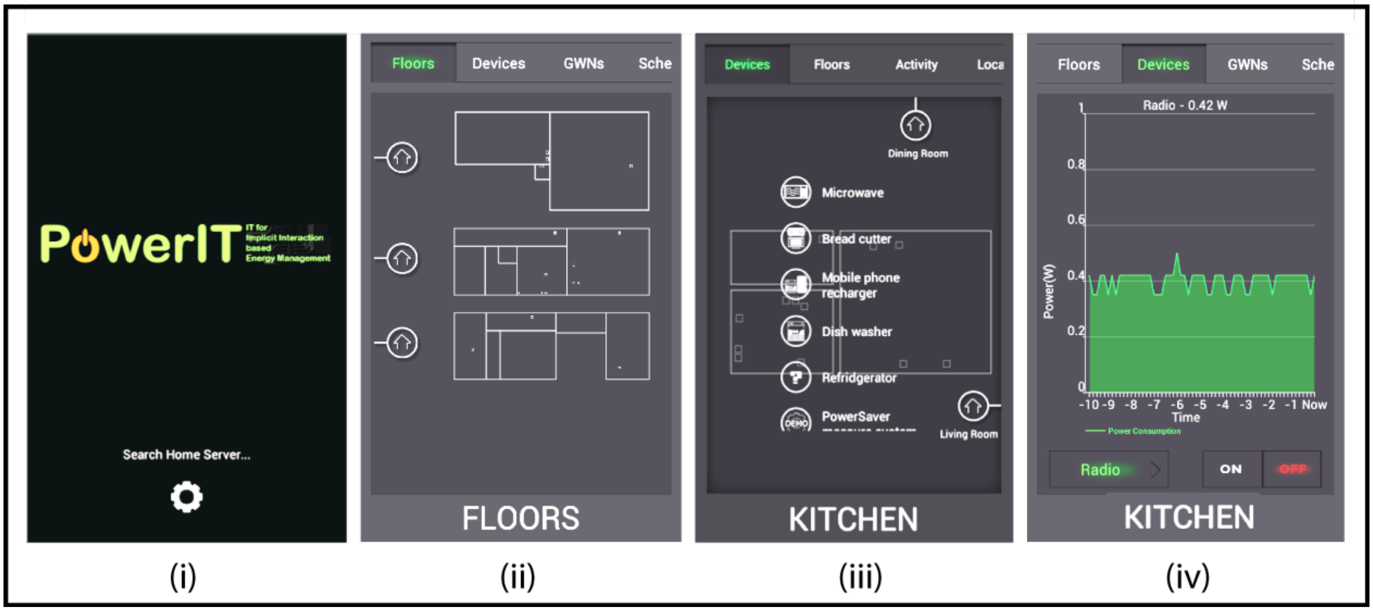


Fig. 3. Developed PowerIT App based on the Android Platform to monitor and control the system. The four views present (i) the starting screen, (ii) the floorplan-view for easy navigation, (iii) the room-view with the assigned energy consumers, and (iv) one selected power consumer (radio) and its realtime power-consumption and power-consumption history (∼ 0.42 Watt).

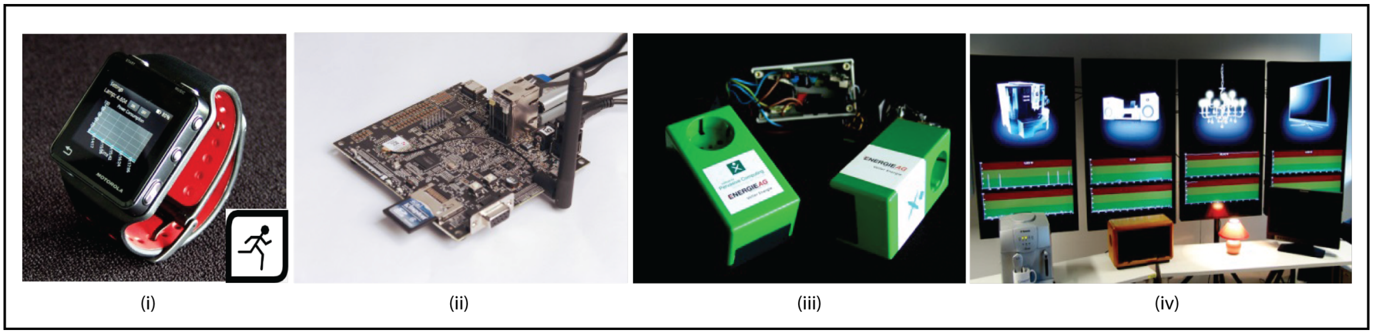


Fig. 4. Demonstration Setup of the PowerIT-System showing (i) MotoACTV Smart-Watch with PowerIT-App and Energy Usage Visualization, (ii) Embedded PandaBoard Platform that hosts the Background Intelligence, (iii) the self-designed Energy Consumer Control Unit and (iv) a demonstration setup with 4 devices (Coffee-Machine, Radio, Lamp, and TV).

using the Energy Consumer control units. The PowerIT-App is deployed on various smart phones and tablets, and a wrist worn smart watch is used as Activity Sensor. These tests were performed for a period of three months before the system was put into action in the field. Four electrical power consumers, a Coffee-Machine, a Radio, a Lamp, and a TV are each connected to an Energy Consumer Control Unit. The Energy Control Unit allows to monitor the power consumption of the connected devices, and offers the ability to turn them on and off. The Energy Consumer control units communicated exclusively using PLC (Power-Line-Communication) with the Background Intelligence System that was hosted on an embedded platform (PandaBoard). As the PandaBoard is not capable of using PLC, we connected it to a Fritz!Powerline 546E to establish the connection. We installed the PowerIT-App on various different Android devices (Nexus 4, Nexus 7, Sony Xperia, Samsung Galaxy SII / III) to test its functionality and stability on different hardware platforms. Tests showed that the functionality and stability was given over all devices. Major differences were only observable in the battery drain rate that can be mostly related back to the different screen sizes that highly influence the power consumption of the mobile devices. Regarding the smart watch that is highly limited in battery capacity, we managed to extend the runtime from around 3 hours with the original firmware, up to 24 hours with a modded firmware and additional optimizations regarding the data transmission intervals and therefore the WiFi-On times. A 24 hour runtime is a good achievement and makes the smart-watch usable for one full day. So, the user can wear it throughout the day, when most of his activities will take place, and can recharge it during the night (while sleeping) where less (and therefore, more predictive) activities are expected to happen.

After performing the previously described tests over a period of three months, that proved the stability and functionality of the system and its components, we installed the system in two households with 3 (man, woman, son) and 4 (man, woman, son, daughter) people in parallel. Both households have 16 devices connected to the system to monitor and control them. A common subset of devices of both are: the microwave oven,

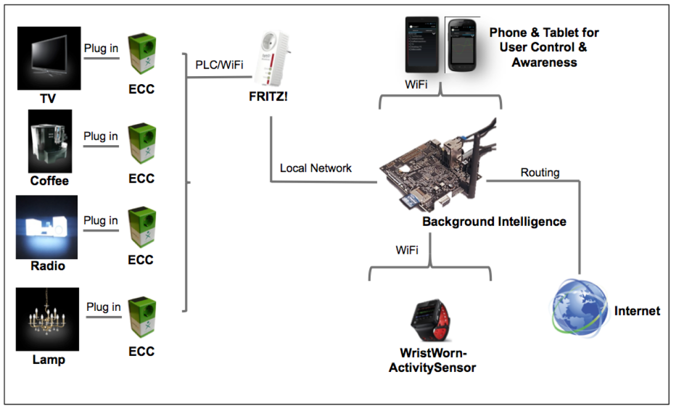


Fig. 5. Schematic of the System Components and their interconnection as used in Figure 4.iv for the demonstration setup.

bread cutter, coffee machine, various lamps, TV, HiFi, radio, the washing machine, deep freezer, fridge, vacuum cleaner, and a multi battery recharger (for, e.g., phones, tablets, etc.). Complementing the fix installed Energy Consumer Control Units, each household got two ’mobile’ ones, that they can use to measure different devices (e.g., eBike, electrical lawn-mower, angle grinder, drill machine, ice cream machine, etc.) on purpose.

Beside the pure technical results of the recorded and annotated datasets containing energy logs and activity data, as exemplarily shown for one week in Figure 6, we also collected preliminary results concerning the question if people have changed, or at least began to change their behavior of using electrical energy in a more effective way. These results are based on interviews we conducted with the people after our system was deployed for four weeks, thus people were aware of their energy consumption during this time. Summarizing these interviews, the main statement was that people realized how many energy their devices consume when they are turned on, or switched to standby mode. The data for standby modes showed that this can range up to 40 Watts for Hifi- or television equipment. People stated that they knew that standby modes consume electrical power but they were not aware of how much. Also devices that do not have an explicit standby mode, such as microwave ovens, were thought by people to consume now power when they are not active. Results showed that also these devices consume a lot of electrical power, e.g., one microwave oven consumed 25 Watts nobody was aware of. This was figured out by people either in realtime, or more systematically in using the electrical energy history logs in the PowerIT-App for single devices, rooms, or floors.

As a result, people immediately used the PowerIT App to disconnect these devices from the power supply resulting in zero use of energy of the disconnected devices. As the users started to be aware of the energy consumption of their devices, regardless if they are used, in standby mode or turned off, they switched through all their devices, and turned the not needed ones off according to their current situation. In doing this, one household who owned the one microwave oven and had three TVs saved up to 60 Watts by just turning these devices off. During the interviewing process, we definitely noticed that people now know the energy consumption of their devices and use them more efficient in terms of energy as they can easily switch not needed power consumers off using the PowerIT-App (as described in more detail in Section III).

The first two households that use the PowerIT system are now online for two months. A brief description of the collected data of the two households that is used for (i) analyzing the behavior of people and their electrical power consumers (e.g., cooling cycles of the fridge) and (ii) for training of activity models, is presented in Table II. This dataset can be used to make the behavior of people more efficient (making them energy-aware) in terms of using electrical energy, as power profiles of devices can be analyzed in detail and presented to people beside the information they get from the PowerIT-App (as shown in Section III).

TABLE II. RECORDED DATA OF THE POWERIT DATASET UNTIL 30. OCTOBER 2013 RESPECTIVELY A PERIOD OF 2 MONTHS THAT IS USED FOR OFFLINE ANALYSIS.

Recordings: Two households, 7 people (2 men, 2 women, 2 boys, 1 girl)
Sensor Recordings: 40 Energy Consumer Control Units at an interval of 10 sec; 7 wrist worn activity sensors with a recording speed of 100Hz.
Sensor Online Time: 40 x 1440h (∼57600h) of energy recordings for single electric power consumers. Activity labels for ∼ 6 x 5 hours/day (300h) (∼1800h)
Recording Size: Energy Recordings 753MB, Activity Recordings 1997MB

Collecting the energy consumption of power consumers and giving technology to people that allows to monitor and control these devices, showed already in the first month to be an effective method to make people aware of their power consumption. Knowing their power consumption, people tended to change their behavior in that way, that not always all devices have to be turned on or in standby mode. Especially the easiness of switching power consumers on and off remotely using a smart gadget and an App made people change their behavior and thinking of how they use electrical energy.

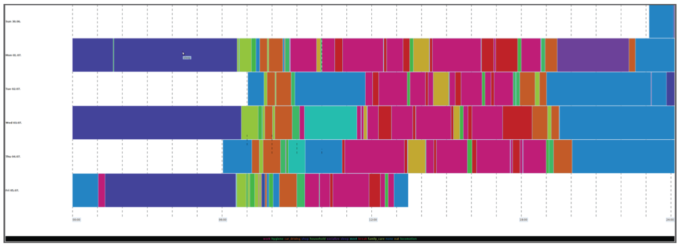


Fig. 6. Activity Traces gathered during a test installation of the system for calendar week 27/2013 for 24/7 yielding to a time use survey with implications to energy management.

To make energy aware behavior even more comfortable, we work on switching from the pure user awareness and explicit control to an implicit control based on the current user activities. Knowing the user activities, electrical power consumers can be switched on- or off automatically without explicitly needed user interaction. To collect the needed activity labels, stating what one user was doing at a specific point in time, according to the recorded energy- and wrist worn sensor data, the smart-watch allows to select the current activity of the user and logs it. This collected metadata is exemplarily shown in Figure 6 for one person for the period of one week. The data was collected for calendar week 27/2013 for 24/7. Each line represents a full 24h day starting with Sunday 30.06-00:00. This recorded activity metadata, in combination with the collected sensor data (energy consumption, accelerometer data from the wrist-worn watch) can be used to train activity recognition models. The color coding for exemplarily selected main activities (not complete) is: *pink*:work, *green*:hygiene, *orange*:car, *violett*:socialize, *dark_blue*:sleep, *light_blue*:don't care, *light_orange*:eat.

Using the activity metadata and the recorded sensor readings, activity recognition models can be trained and evaluated to be further used to implicitly control electrical power consumers based on an Energy Management Rule Set. This frees people to explicitly turn power consumers on and off and can make energy saving even more comfortable.

V. Conclusion

Within this paper we have presented and evaluated the use of smart gadgets (i.e., smart-phones, tablets, and watches) to make people aware of their energy consumption. We designed the PowerIT System that permanently collects the energy consumption from connected devices. We developed the PowerIT-App based on the Android Platform that can be used by people on different gadgets to monitor and control the energy consumption of the connected devices. We deployed the PowerIT system in two households with 3 (man, woman, son) and 4 (man, woman, son, daughter) people in parallel, and in sum 40 connected electrical power consumers for a period of two months. Using the PowerIT system to monitor their electrical devices in realtime, turning them on- and off remotely, and additionally showing energy history logs made people aware of how many electrical energy is consumed by their devices. Interviewing the participants showed that already in the first four weeks of the test installation, gaining awareness about the power consumption of their electrical devices, people changed their behavior to a more attentive use of electrical energy. People used their phones, tablets and smart-watches to check if their currently not used devices were turned on and switched them off. This resulted in a more efficient use of energy as only devices were turned on that were needed at the specific point in time. The fact that the PowerIT system works completely autonomous and uses already deployed smart gadgets for monitoring and control of the system, like smart phones and tablets, the system can be used without affecting the level of living of people. Although the behavioral change of people towards a more energy aware and efficient behavior was already noticeable after four weeks, the future will see an implicit control of power consumers based on inferred user activities. To address this issue, we additionally collect activity labels using a smart watch that will provide the necessary information to train activity recognition models for the future implicit energy management approach.

Acknowledgment

The project OPPORTUNITY acknowledges the financial support of the Future and Emerging Technologies (FET) programme within the Seventh Framework Programme for Research of the European Commission, under FET-Open grant number: 225938.
The project PowerIT acknowledges the financial support of the FFG FIT-IT under grant number: 830.605.

References

[1] U.S. Energy Information Administration (EIA), "International Energy Outlook 2013," July 2013.

[2] G. Hoelzl *et al.*, "Locomotion@location: When the rubber hits the road," in *The 9th International Conference on Autonomic Computing (ICAC2012), San Jose, California, USA*, September 2012, pp. 73–78.

[3] D. Salber, A. K. Dey, and G. D. Abowd, "The context toolkit: aiding the development of context-enabled applications," in *Proceedings of the SIGCHI conference on Human factors in computing systems: the CHI is the limit*, ser. CHI '99. New York, NY, USA: ACM, 1999, pp. 434–441.

[4] M. Keally, G. Zhou, G. Xing, J. Wu, and A. Pyles, "Pbn: towards practical activity recognition using smartphone-based body sensor networks," in *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*, ser. SenSys '11. New York, NY, USA: ACM, 2011, pp. 246–259.

[5] I. Nordin, P. Chee, M. Addi, and F. Harun, "Ez430-chronos watch as a wireless health monitoring device," in *5th Kuala Lumpur International Conference on Biomedical Engineering 2011*, ser. IFMBE Proceedings, N. Osman, W. Abas, A. Wahab, and H.-N. Ting, Eds., vol. 35. Springer Berlin Heidelberg, 2011, pp. 305–307.

[6] A. Sellen, Y. Rogers, R. Harper, and T. Rodden, "Reflecting human values in the digital age," *Commun. ACM*, vol. 52, no. 3, pp. 58–66, Mar. 2009.

[7] P. Ebinger, J. Hernández Ramos, P. Kikiras, M. Lischka, and A. Wiesmaier, "Privacy in smart metering ecosystems," in *Smart Grid Security*, ser. Lecture Notes in Computer Science, J. Cuellar, Ed., vol. 7823. Springer Berlin Heidelberg, 2013, pp. 120–131.

[8] U. Greveler, B. Justus, and D. Loehr, "Forensic content detection through power consumption," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 6759–6763.

[9] A. A. Salah, B. Lepri, A. S. Pentland, and J. Canny, "Understanding and changing behavior," *Pervasive Computing, IEEE*, vol. 12, no. 3, pp. 18–20, 2013.

[10] B. Fogg, "A behavior model for persuasive design," in *Proceedings of the 4th International Conference on Persuasive Technology*, ser. Persuasive '09. New York, NY, USA: ACM, 2009, pp. 40:1–40:7.

[11] L. Bao and S. Intille, "Activity recognition from user-annotated acceleration data," in *Pervasive Computing*, ser. Lecture Notes in Computer Science, A. Ferscha and F. Mattern, Eds. Springer Berlin Heidelberg, 2004, vol. 3001, pp. 1–17.

[12] E. Tapia, S. Intille, and K. Larson, "Activity recognition in the home using simple and ubiquitous sensors," in *Pervasive Computing*, ser. Lecture Notes in Computer Science, A. Ferscha and F. Mattern, Eds. Springer Berlin Heidelberg, 2004, vol. 3001, pp. 158–175.

[13] J. Ward, P. Lukowicz, G. Troster, and T. Starner, "Activity recognition of assembly tasks using body-worn microphones and accelerometers," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 28, no. 10, pp. 1553–1567, 2006.

[14] G. Hoelzl, M. Kurz, and A. Ferscha, "Goal oriented recognition of composed activities for reliable and adaptable intelligence systems," *Journal of Ambient Intelligence and Humanized Computing (JAIHC)*, p. in Press, July 2013.

[15] M. Kurz *et al.*, "The opportunity framework and data processing ecosystem for opportunistic activity and context recognition," *International Journal of Sensors, Wireless Communications and Control, Special Issue on Autonomic and Opportunistic Communications*, pp. 102–125, December 2011.

[16] G. Hoelzl, M. Kurz, and A. Ferscha, "Goal processing and semantic matchmaking in opportunistic activity and context recognition systems," in *The 9th International Conference on Autonomic and Autonomous Systems (ICAS2013)*, March 2013, pp. 33–39.

[17] E. Garcia-Ceja and R. Brena, "Long-term activity recognition from accelerometer data," *Procedia Technology*, vol. 7, no. 0, pp. 248 – 256, 2013.

[18] S. Belgaonkar, E. Elavarasi, and G. Singh, "Smart lighting and control using msp430 & power line communication," *International Journal Of Computational Engineering Research*, vol. 2, no. 3, pp. 662–666, 2012.

Towards Temporal Saliency Detection: Better Video Understanding for Richer TV Experiences

Joël Dumoulin, Elena Mugellini, Omar Abou Khaled
Department of Information Technologies
HES-SO, Fribourg, Switzerland
joel.dumoulin@hes-so.ch
elena.mugellini@hes-so.ch
omar.aboukhaled@hes-so.ch

Marco Bertini, Alberto Del Bimbo
Media Integration and Communication Center (MICC)
University of Florence, Italy
bertini@dsi.unifi.it
delbimbo@dsi.unifi.it

***Abstract*—More and more popular, Smart TVs and set-top boxes open new ways for richer experiences in our living rooms. But to offer richer and novel functionalities, a better understanding of the multimedia content is crucial. If many works try to automatically annotate videos at object level, or classify them, we think that investigating the emotions through the use of digital analysis and processing techniques will allow great TV experience improvements. With our work, we propose a temporal saliency detection approach capable of defining the most exciting parts of a video that will be of the most interest to the users. To identify the most interesting events, without performing their classification (in order to be independent from the video domain), we compute a time series of arousal (excitement level of the content), based on audio-visual features. Our goal is to merge this preliminary work with user emotions analysis, in order to create a multi-modal system, allowing to bridge the gap between users' needs and multimedia contents.**

Keywords-Digital Analysis and Processing; Temporal Saliency; Affective Content Analysis; Arousal Modelling; Emotions

I. Introduction

Development of Smart TV devices has been ongoing for many years - first patent in 1994, first real attempt at its production (by Microsoft and Thomson) in 2000 - and now it is becoming a commercial reality. Samsung and LG for instance are pushing their new devices, with advanced features such as voice or gesture based control, and embedded recommender systems. Other actors that are not TV manufacturer also propose to bring the Smart TV experience to living rooms without the need to buy a new TV, with set-top boxes. Despite the limited success of the Google TV (launched in 2010), these devices are becoming more and more popular (e.g., Apple TV).

In order to propose to the user richer experiences with these Smart TVs, it is crucial to better understand not only the user itself, considering for example his interests, but also the content. Bridging the gap between users and multimedia content would allow to propose innovative features, and also improve recommender systems [1]. This represents the starting point of our work: we want to create richer TV user experiences. To this end we need automatic multimedia annotation systems, e.g., to create personalized access to video content, according to user preferences. In particular, we want to explore emotions, because we believe that they play a central role in the user TV experience. Detection of emotions can be done with two points of view: analysis of user emotions and analysis of emotions contained in a video [2][3]. Our goal is to build a multi-modal system, capable of combining the two perspectives, because we think that understanding well what the multimedia content represents in terms of emotions, and what the user is feeling while watching the movie, will allow us to close the distance between user needs and the multimedia content, and to provide new experiences into the living rooms.

In this paper, we propose a temporal saliency approach, capable of detecting the exciting parts of a movie, based on an arousal curve. The rest of the paper is organized as follows. A state of the art for the affective content analysis is presented in Section 2. Our temporal saliency approach is introduced in Section 3. Section 4 details the arousal curve generation. Section 5 presents our preliminary results. Finally, we define our research agenda in Section 6, and conclusions are drawn in Section 7.

II. Related work

Content-based multimedia information retrieval research provides new methods and techniques to search the ever increasing amount of multimedia content [1], and many of them have potential implications in the Smart TV world.

Video summarization is one key aspect in video management. It not only allows to better understand the dynamic of the movie, but also to improve its browsing and navigation. Many works try to focus on the user, for instance by building user centric models [4] or directly by analyzing the user physiological responses [5]. Another approach is to focus on the multimedia content itself, for instance by detecting audiovisual saliency [6].

Computer systems capable of detecting user emotions would have many interesting applications in human-computer interaction area, but also represent an interesting approach to extract the interesting parts of a video, if we define them as the parts that bring emotion to the user. It is possible to focus on the user [3][7], but also on the multimedia content itself. Detecting user emotions is not only very dependent to the user observed, as emotion is a subjective reaction, but it is also an information not available when the video content is produced. To overcome this problem, Hanjalic et al. [2][8] proposed to extract and model the affective content of the video, and this approach is called “Affective content analysis”. The affective content is defined as the intensity and type of emotion expected to arise in the user while watching an image or a video. Wang et al. [9] proposed a set of affective categories and steps for their classification, in order to improve this affective understanding approach in films. Lu et al. [10] investigated how shape features are related to emotions aroused from images in human beings, by analyzing many characteristics such as roundness, angularity, simplicity, complexity, etc. Zhang et al. [11] propose to take advantage of the affective analysis in order to improve movie browsing, and define rich audio-visual features. Recently, Wang et al. [12] achieved soccer highlight extraction by modelling affection arousal based on both visual and audio arousal related features: sound energy, shot cut density, shot intensity and replay, the highlights being extracted based on the arousal curve crests detected. Benini et al. [13] propose to overcome the subjective sphere of emotions, by shifting the representation towards the connotative properties of movies, in a space inter-subjectively shared among users, allowing to define, relate and compare affective descriptions of films.

If affective content analysis approaches are interesting for highlight extraction, particularly for sport videos, they need to be improved and adapted to films, in order to automatically detect the parts that will be of the most interest to the users.

III. Temporal saliency detection

In our work, we want to define important parts in movies as the parts that are salient regarding the others. This idea is inspired from the work of Itti et al. [14] about saliency-based visual attention determination (bottom-up approach), where the idea is to generate a saliency map for a single image - which topographically codes for local conspicuity over the entire visual scene - in order to define where there is something interesting to look at. Our idea is to adapt this approach into a temporal saliency detection specific to video content. The result is not “where” to look at, but “when” to look at. It is similar to Otsuka et al. [15] proposition of a sports highlights detection function by using audio features, based on “commentator’s excited speech” identification. While many works are done around the concept of saliency [16], and also spatiotemporal saliency [17], very few address this idea of temporal saliency in videos.

The approach we chose in order to detect this temporal saliency is based on the emotions that these parts could arouse to the user watching the movie, and particularly the excitement, defined as the arousal. We plan to take also in account the type of the emotion (valence). The schema of our system is illustrated in Fig. 1. It shows the different processing steps that are planned to be implemented, in order to extract the needed elements (visual excitement, audio excitement, etc.) from the video and the audio streams, to depict the excitement (arousal) and the type of the emotion (valence).

Our approach is in some aspect close to highlight extraction techniques. But, while highlight extraction techniques try to summarize the movie, with our temporal saliency approach we try to find the parts of the movie that will be exciting for a particular user profile (from an emotional point of view). In regards to this, our approach is different from highlight extraction. As shown in Fig. 1, we use several features in order to compute the temporal saliency. Some are extracted from the video stream, and the others from the audio stream. It is crucial to use both streams, as they both convey important emotion and excitement information. The processing of those features will allow us to understand the two main affective axes of the multimedia content: the arousal and the valence, needed to define the temporally salient parts of the video.

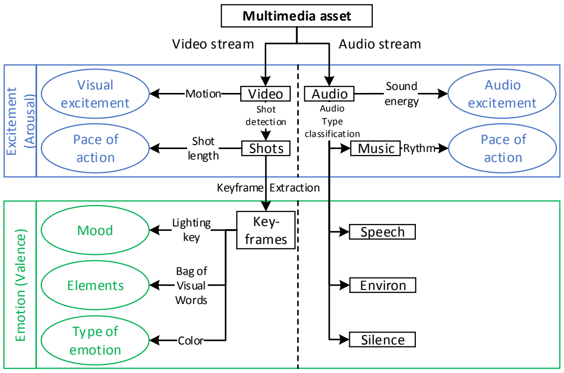


Figure 1. Multimedia asset processing schema. Video and audio streams are processed to extract information about the conveyed excitement and emotion.

IV. Arousal curve generation

As a starting point, we chose two features: shot intensity and sound energy. The shot intensity gives the pace of action, while the sound energy gives the audio excitement. These two features allow us to compute an arousal curve. Finally, we apply a crest generation algorithm on it to detect the most exciting parts of the video.

A. Shot intensity

We detect only hard cuts. As we want to define parts of the movie where there is a high shot intensity, corresponding to high arousal parts, detecting hard cuts is sufficient. As gradual transitions are more used to conclude a scene, it does not means a lot for high shot intensity detection. We chose the Edge Change Ratio (ECR) technique, as it is a good compromise between accuracy and implementation complexity [18]. Our implementation is based on the ECR algorithm proposed by Lienhart [19], but with a small tweak. Usually, a motion compensation step is done in order to compensate small linear movements between two consecutive frames. Instead, we use this idea of calculating the transformation needed to go from one frame to its following, but we calculate it only when the system triggers a shot cut, as a change quantification. Based on a threshold, this change amount value allows us to remove false positives: if the change is small, it is certainly a false positive, but if this value is relatively big, it is certainly a true positive. As we estimate the transformation matrix only when we detect shots and not for every consecutive frames (plus we do not need to apply the transformation), this approach is more efficient, and gives similar results to the standard algorithm. Finally, the shot cut density is computed as proposed by Wang et al. [12]:

$$c(k) = e^{(1-n(k))/r} \tag{1}$$

where *n(k)* is the number of frames including the *k-th* video frame and *r* is a constant determining the distribution of the values.

B. Sound energy

The sound conveys a big part of the emotion of a movie. While several features could be used (music rhythm, etc.), we use the sound energy as our sound feature. We computed the sound energy as described by Wang et al. [12] as:

$$e(k) = \sum_{i=1}^{N} x(i)^2 \tag{2}$$

where *e(k)* is the sound energy at *k-th* frame, *x(i)* is *i-th* sample point value in audio frames, *N* is the number of audio frames.

C. Crests generation

We followed approach proposed by Wang et al. [12] for the crests generation. First, the raw features are normalized and smoothened with a Kaiser window [20]. Then, we used a linear weighted summarization to merge our two features together. After the fusion, the resulting signal is again smoothened and normalized. Finally, the crests are detected with a sliding window based algorithm, and filtered regarding its fluctuant amplitude. We obtained the best results with values of 10 samples for the window size, 3 samples for the window step, and 0.1 for the crest intensity threshold used to filter the insignificant crests. We need to define with future experimentations if these values are depending on the movie type.

V. Preliminary results

We planned to test our system on the Emotional Movie Database (EMDB) [21], but, unfortunately, it does not come with sound, and we need it in order to compute the sound energy. Instead, we use the Schafer et al. dataset [22], that is composed of a total of 70 film excerpts, representing 7 *a priori* emotional categories: anger, sadness, fear, disgust, amusement, tenderness, and neutral state. It allows us to test our system on different movie styles and categories (black and white, color, horror, comedy, etc.).

Figs. 2, 3, and 4 show the result we obtained by processing one of the movie excerpts. The scene is part of the amusement category. It lasts 2'09", showing "Jacquouille" and Godfroid destroying the postman's car, in the famous French movie "The Visitors". The x-axis corresponds to the frame number. Fig. 2 represents the raw features for the sound and the video streams. The result of the preprocessing step (normalization and smoothing with a Kaiser windows) is shown in Fig. 3. Finally, Fig. 4 is the resulting arousal curve, after the fusion of the two pre-processed features, again normalized and smoothened. The vertical dashed lines are the detected crests, and the two interesting events of the sequence are manually annotated in green.

During this scene, there are two particular events where there is an arousal peak: 1) when the car breaks and stop just in front of "Jacquouille", 2) when "Jacquouille" and Godfroid destroy the postman's car. In these two particular events, there is an increase of the sound energy and the shot cut density, and this is clearly noticeable on the plots. The result is that the arousal curve and the crest detection clearly correspond to these two particular events, and this is a really promising result. We still need to improve our system in order to automatically define these parts around the crests (start and end times).

In order to ease results analysis, we have built a web application, allowing us to navigate through the movie and the arousal curve in a convenient way. We can easily go to a particular point of the arousal curve and it automatically seek the movie accordingly. This is helping us to control if the results are coherent with the movie, until we have a ground truth, since it is not available for the dataset we used.

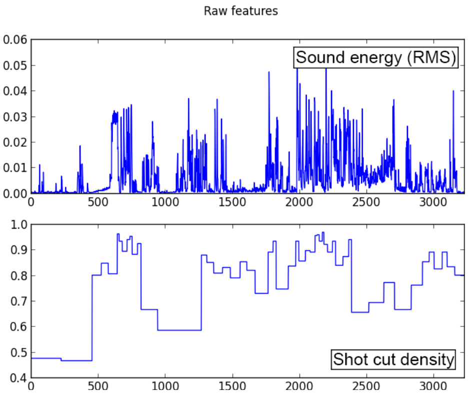


Figure 2. Raw features - Sound energy plot is above (root mean square of the audio stream's sound energy computation), shot cut density is below.

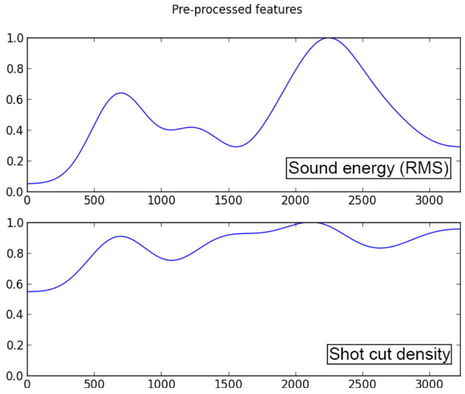


Figure 3. Pre-processed features - Features are normalized and smoothened (with a Kaiser window). Sound energy plot is above, shot cut density is below.

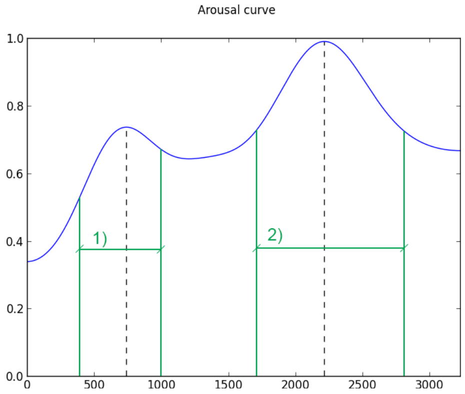


Figure 4. Arousal curve - Arousal curve, resulting from the fusion of the pre-processed features, again normalized and smoothened.

VI. Research agenda

There are several steps planned next. We first need to validate our system. This step is a challenging one, because, as far as we know, there are currently no datasets containing the meta data we need to constitute a usable ground truth. Indeed, datasets like EMDB [21] and Schaefer et al. [22] only provide emotional values (arousal, valence) for the whole video sequence in order to classify it in one emotional category. We plan to use MAHNOB-HCI [23], that is a multimodal database recorded in response to affectively stimulating excerpts from movies, over 27 participants. Similarly to the Schafer et al. dataset [22] that we used to conduct our first tests, the movies excerpts cover six main emotional categories: disgust, amusement, joy, fear, sadness, neutral. If different recorded modalities are provided (e.g., facial expressions, audio signals, eye gaze data), we would like to use as a starting point the physiological responses (e.g., electrocardiography, respiration amplitude, skin temperature) in order to generate an arousal curve, that will constitute our ground truth. It will allow us to validate our system, and compare it with other approaches.

Then, in order to improve our system, we plan to add other features. We think that motion analysis will be a good feature to start with, as it depicts well the dynamic of a movie. Once the arousal part validated, we could address the valence part, by analyzing the key-frames allowing to extract the mood, as one of the key aspect that describes the type of the emotion conveyed. Another interesting task would be to have different granularity levels for the emotionally interesting parts of the video. This idea would be to define which parts are interesting at the movie level, or at the chapter level, or at the scene level.

Adapting the curve generation according to the movie type would be an interesting task. This would allow our system to perform well with different movie types and to recognize subcategories of movies (e.g., subtypes of Westerns: Classical Westerns, Spaghetti Westerns, etc.), by using the generated emotional curves as input features for the classification.

VII. Conclusion

We presented our current work, focused on a temporal saliency detection approach in order to define exciting parts of a movie. We think that addressing this task with an emotional point of view can better meet the user needs than with a traditional highlight extraction approach. We presented our method for the arousal curve generation. We also presented a tweak of the Edge Change Ratio (ECR) technique for shot boundary detection. Our goal is to merge our multimedia centric approach, with a user centric approach, based on user emotions detection. This would constitute a multi-modal system, capable of bridging the gap between the users and the multimedia content they access through Smart TVs. Finally, this system will allow us to realize our ideas of new features for Smart TVs, e.g., enhanced recommendation systems matching user mood, and user attention based advanced features like indication to the user that a particularly interesting part of the movie will be missed because he is doing something else.

References

[1] M. S. Lew, N. Sebe, C. Djereba, and R. Jain, “Content-Based Multimedia Information Retrieval : State of the Art and Challenges,” ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP), vol. 2, no. 1, 2006, pp. 1–19.

[2] A. Hanjalic, “Extracting moods from pictures and sounds: Towards truly personalized TV,” Signal Processing Magazine, IEEE, no. March 2006, 2006, pp. 90–100.

[3] M. Soleymani, G. Chanel, J. J. Kierkels, and T. Pun, “Affective ranking of movie scenes using physiological signals and content analysis,” Proceedings of the 2Nd ACM Workshop on Multimedia Semantics, 2008, pp. 32–39.

[4] Y.-f. Ma, X.-s. Hua, L. Lu, and H.-j. Zhang, “A generic framework of user attention model and its application in video summarization,” IEEE Transactions on Multimedia, vol. 7, no. 5, Oct. 2005, pp. 907–919.

[5] A. G. Money and H. Agius, “Analysing user physiological responses for affective video summarisation,” Displays, vol. 30, no. 2, Apr. 2009, pp. 59–70.

[6] G. Evangelopoulos, “Movie summarization based on audiovisual saliency detection,” in Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on, 2008, pp. 2528–2531.

[7] Z. Zeng, M. Pantic, G. I. Roisman, and T. S. Huang, “A survey of affect recognition methods: audio, visual, and spontaneous expressions.” IEEE transactions on pattern analysis and machine intelligence, vol. 31, no. 1, Jan. 2009, pp. 39–58.

[8] A. Hanjalic and L. Xu, “User-oriented affective video content analysis,” Content-Based Access of Image and Video Libraries, 2001. (CBAIVL 2001). IEEE Workshop on, 2001, pp. 50–57.

[9] H. L. Wang and L.-f. Cheong, “Affective understanding in film,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 6, Jun. 2006, pp. 689–704.

[10] X. Lu, P. Suryanarayan, R. A. Jr, J. Li, M. G. Newman, and J. Wang, “On shape and the computability of emotions,” in Proceedings of the 20th ACM international conference on Multimedia - MM ’12, 2012, pp. 229–238.

[11] S. Zhang, Q. Tian, and Q. Huang, “Utilizing affective analysis for efficient movie browsing,” in Image Processing (ICIP), 2009 16th IEEE International Conference on, no. 49, 2009, pp. 1853–1856.

[12] Z. Wang, J. Yu, Y. He, and T. Guan, “Affection arousal based highlight extraction for soccer video,” Multimedia Tools and Applications, Jul. 2013, pp. 1–28.

[13] S. Benini, L. Canini, and R. Leonardi, “A Connotative Space for Supporting Movie Affective Recommendation,” Multimedia, IEEE Transactions on, vol. 13, no. 6, 2011, pp. 1356–1370.

[14] L. Itti, C. Koch, and E. Niebur, “A Model of Saliency-Based Visual Attention for Rapid Scene Analysis,” Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 20, no. 11, 1998, pp. 1254–1259.

[15] I. Otsuka and K. Nakane, “A highlight scene detection and video summarization system using audio feature for a personal video recorder,” Consumer Electronics, IEEE Transactions on, vol. 51, no. 1, 2005, pp. 112–116.

[16] A. Toet, “Computational versus psychophysical bottom-up image saliency: a comparative evaluation study,” IEEE transactions on pattern analysis and machine intelligence, vol. 33, no. 11, Nov. 2011, pp. 2131–46.

[17] C. Guo and L. Zhang, “A novel multiresolution spatiotemporal saliency detection model and its applications in image and video compression.” Image Processing, IEEE Transactions on, vol. 19, no. 1, Jan. 2010, pp. 185–98.

[18] A. Smeaton, P. Over, and A. Doherty, “Video shot boundary detection: Seven years of TRECVid activity,” Computer Vision and Image Understanding, vol. 114, no. 4, 2010, pp. 411–418.

[19] R. Lienhart, “Reliable Transition Detection in Videos : A Survey and Practitioner s Guide,” International Journal of Image and Graphics, vol. 01, no. 03, 2001, pp. 469–486.

[20] F. Harris, “On the use of windows for harmonic analysis with the discrete fourier transform,” Proceedings of the IEEE, vol. 66, no. 1, Jan 1978, pp. 51–83.

[21] S. Carvalho, J. Leite, S. Galdo-Álvarez, and O. F. Gonçalves, “The Emotional Movie Database (EMDB): a self-report and psychophysiological study.” Applied psychophysiology and biofeedback, vol. 37, no. 4, Dec. 2012, pp. 279–94.

[22] A. Schaefer, F. Nils, X. Sanchez, and P. Philippot, “Assessing the effectiveness of a large database of emotion-eliciting films: A new tool for emotion researchers,” Cognition & Emotion, vol. 24, no. 7, Nov. 2010, pp. 1153–1172.

[23] M. Soleymani, J. Lichtenauer, T. Pun, and M. Pantic, “A multimodal database for affect recognition and implicit tagging,” Affective Computing, IEEE Transactions on, vol. 3, no. 1, 2012, pp. 42–55.

A Dependency Parsing Method Based on the Hierarchical Structure in Japanese Language

Kazuki Ono

Graduate School of Culture and Information Scicence
Doshisha University
1-3 Tatara-Miyakodani, Kyotanabe, Kyoto, 610–0394, Japan
Email: ono@ilab.doshisha.ac.jp

Kenji Hatano

Faculty of Culture and Information Scicence
Doshisha University
1-3 Tatara-Miyakodani, Kyotanabe, Kyoto, 610–0394, Japan
Email: khatano@mail.doshisha.ac.jp

Abstract—**In this paper, we propose a new statistical dependency parsing method in Japanese language based on an extended hierarchical language model. Conventional Japanese statistical dependency parsers are primarily based on the bi-nominal dependency model between phrases, which has a limitation related to the order of phrases. Accordingly, the length of the phrase, which depends of dependency is limited by this limitation, the model is lacking. We propose a dependency model in Japanese language that considers the order of phrases based on the hierarchical Pitman-Yor process in order to overcome this limitation. Consequently, compared with conventional methods, our method can parse dependencies in long and complex Japanese sentences relatively well.**

Keywords-Dependency Parsing; Syntax Analysis; Syntax Tree Modeling

I. INTRODUCTION

Asian languages are based on case grammar and in many of them, sentences are composed in the order subject, object, and verb (SOV), giving rise to them being termed SOV languages. Japanese has the same characteristics; however, its phrase order is relatively unfettered.

In English, the syntactic function of each phrase is represented by phrase order, while in Japanese, postpositions represent the syntactic function of each phrase. Further, phrases that comprise one or more postpositions following a noun, which play a similar role to declension of nouns, have been devised and used to syntactically analyze Japanese sentences.

Hence, it may be said that syntactic analysis is equivalent to parsing dependencies between phrases. This is because the semantic rules of Asian languages are explained as relationships of phrases. As a result, conventional dependency parsing methods in such languages utilize the bi-nominal dependency model to decide whether a dependency relation exists between pairs of phrases or not [1]–[3].

In the syntactic analysis used for English, on the other hand, Tree Substitution Grammar (TSG) has attracted attention as a language model [4]. TSG helps to establish the highest accuracy of English parsing, including hierarchical structure, by learning the rewrite rules of any depth [5], [6].

The hierarchical structure is defined as a set of rewriting rules of Context Free Grammar (CFG). Syntax trees generated by TSG describe the order of phrases, whereas those generated by case grammar only represent relationships between phrases. In short, the syntax trees generated by TSG not only have the relationships between phrases but also the orders of phrases, so that they may facilitate precise extraction of dependencies between phrases.

Incidentally, the syntax trees from case grammar are generated based on the bi-nominal model [1], [2]. As a consequence, the order of phrases in these syntax trees do not include a hierarchical structure. They are instead subject to constraints related to the constant order of phrases. As a result, dependency parsing of Asian languages using the bi-nominal dependency model is not very successful. We believe that the accuracy of dependency parsing of Asian languages can be improved by applying TSG to them. Consequently, in this paper, we propose a dependency parsing method in Japanese language based on TSG that considers the syntax tree with context dependency.

Our method is characterized by the handling of exchangeable sequence of phrases in case grammar to utilize the extracted hierarchical structure using TSG. That is, we can generate a dependency parsing model by calculating the probabilities of integrating phrase dependencies from supervised training data with a hierarchical structure. Thus, it can be said that our approach is a novel dependency parsing method in Japanese language with hierarchical structure relations because of the way it handles the relationships of each of the phrase dependencies.

II. BASIC PROCESSES

In this section, we discuss the basic processes used in our research. These are, specifically, the Pitman-Yor process [7] and its extension called the Hierarchical Pitman-Yor process [8], which we use to generate a syntax tree model based on TSG [5].

A. The Pitman-Yor Process

The Pitman-Yor process is a non-parametric Bayesian model [7]. In natural language processing, it is used to generate an n-gram model. It is a stochastic process that generates an infinite discrete probability distribution G, and is denoted by $\text{PY}(d, \theta, G_0)$. $\text{PY}(d, \theta, G_0)$ has three parameters: d is a discount parameter with $0 \leq d \leq 1$, θ is a strength parameter that meets the condition $\theta \geq -d$, and G_0 is a base distribution over a probability space. In natural language processing, the probability space is usually generated from the probabilities of phrase occurrences.

When d is zero, $\text{PY}(d, \theta, G_0)$ becomes the Dirichlet process, denoted $\text{DP}(\theta, G_0)$. In short, because $\text{DP}(\theta, G_0)$ can generate an infinite dimensional Dirichlet distribution, $\text{PY}(d, \theta, G_0)$ can also support it. As outlined above, d is a concentration parameter for G_0; therefore, we can define the following equation:

$$G \sim \text{PY}(d, \theta, G_0) \tag{1}$$

That is, $\text{PY}(d, \theta, G_0)$ is an extended version of $\text{DP}(\theta, G_0)$. Let W be a fixed and finite vocabulary of V phrases. The Pitman-Yor process generates for each phrase $w \in W$ a vector of phrase probabilities $G(w)$. $\text{DP}(\theta, G_0)$ is approximated by Dirichlet distribution $Dir(\theta G_0(w_1), \ldots, \theta G_0(w_i), \ldots, \theta G_0(w_r))$ that expresses any division of the disintegration space for which the size of the phenomenon space is r in observing any phrase w_i as follows:

$$\text{DP}(\theta, G_0) \sim Dir(\theta G_0(w_1), \ldots, \theta G_0(w_i), \ldots, \theta G_0(w_r)) \tag{2}$$

Here, $G_0(w_i)$ is an integral of the base distribution G_0, therefore it is equal to the sum of the probabilities of phrase occurrences in the disintegration space. In short, we can say that the Pitman-Yor process is a recursive stochastic process whose input is a set of phrases w_i and base distribution is G_0.

In general, these procedures for generating n-gram distribution drawn from G are often referred to as the Chinese restaurant process [9]. In the Chinese restaurant process, we fancifully imagine a restaurant with an infinite number of tables whose capacities are infinite. The existing distribution of customers (phrases) who come to the restaurant and the tables (discount strength) with one by one dish (phrase vocabulary) is based on the n-gram model, denoted by G, and the hypothesis to the tables elicits the base distribution G_0. The customers are compared to phrases in the Pitman-Yor process, such that a customer continues to sit at the same table if the customer coming to the restaurant is that same customer. However, if it is another customer that had not previously entered the restaurant, the customer sits down at a new table. Given this scenario, we can formulate the Pitman-Yor process as (3):

$$\text{PY}(d, \theta, G_0) = \frac{c_k - d}{\theta + c_\cdot} + \frac{\theta + dt}{\theta + c_\cdot} p(w_k) \tag{3}$$

where t is the number of customers under the base distribution G_0, c_k is the number of species, $c_\cdot$ is the total number of customers, and $p(w_k)$ is the probability of a customer visiting the restaurant. Here, the parameters d and θ is in the Pitman-Yor process are non-parametric. Therefore, we have to generate the distribution approximated by the base distribution G_0 with these parameters using a Gibbs sampling algorithm, such as Markov Chain Monte-Carlo [9].

B. The Hierarchical Pitman-Yor Process

The Hierarchical Pitman-Yor process [8] is a stochastic process that is based on a hierarchical extension of the Pitman-Yor process. An n-gram language distribution over which the current phrase is given various context $\mathbf{u}$, consisting of up to $(n-1)$ phrases, can be described by the Hierarchical Pitman-Yor process. Consequently, an n-gram distribution G_u is generated by the Pitman-Yor process using the base distribution $G_{\pi(u)}$, which is generated in the given context $\mathbf{u}$ as follows:

$$G_{\mathbf{u}} \sim \text{PD}(d_{\pi|\mathbf{u}|}, \theta_{\pi|\mathbf{u}|}, G_{\pi(\mathbf{u})}) \tag{4}$$

where strength and discount parameters are calculated on the basis of the length of context $\mathbf{u}$, $\pi(\mathbf{u})$ is the suffix of $\mathbf{u}$ consisting of all but the earliest phrase, and $G_{\pi(\mathbf{u})}$ is a vector of probabilities of its context.

When we recursively place a stochastic process such as $G_{\pi(\pi(\mathbf{u}))}$ over $G_{\pi(\mathbf{u})}$ using (4), we can define a stochastic process that generates the n-gram distribution. This process is repeated until we get G_ϕ as the base distribution, the vector of probabilities over the current phrase given the empty context ϕ.

As described above, the structure of the stochastic process generated by the hierarchical Pitman-Yor process is expressed as a suffix tree with depth n.

Each node in the suffix tree corresponds to a context consisting of up to $(n-1)$ phrases, and each child corresponds to the addition of a different word to the beginning of the context. The Hierarchical Pitman-Yor process can generate an n-gram language model precisely as demonstrated in the language model based on Kneser–and–Ney smoothing [10].

III. Related Work

In this section, we first discuss a conventional dependency parsing method in Japanese language and its limitations. We then look at how TSG obtains highly precise English language parsing with a hierarchical structure, and examine its application to the parsing of dependencies in the Japanese language.

A. Dependency Parsing based with the Bi-nominal Model

The Bi-nominal approaches, which generate syntax trees, are the conventional approaches used to parse dependencies between phrases in Japanese language [1], [3]. They generate a syntax tree model whether there is a dependency in Japanese language between phrases or not based on features like part of speech, inflectional form, and so on, and conduct syntactic analysis using the generated syntax tree based on the following algorithm:

1) Check all the phrases in a sentence to ascertain whether they have a dependency with others located on the right side of the syntax tree.
2) Designate any phrase that has a dependency in Step 1 as the analysis result. At this time, the referrer of the dependency is excluded from the target of Step 1.

3) Repeat Steps 1 and 2 and keep the analysis results until all but the final phrase has a dependency.

Conventional methods based on the bi-nominal model do not consider the features of only the relationship between two phrases in a sentence. They misjudge some of the dependencies shown in Figure 1.

There is a Japanese sentence “トムはこの本をジムを見た女性に渡した” in Figure 1. This sentence contains a complex structure. The meaning of the sentence in English is “Tom gave this book to a woman who saw Jim.” in English. Originally, the phrase “本を (the book)” has to take the dependency depicted by the dashed line to another phrase “渡した (gave)”, because “the book” becomes the object of “gave”. However, sometimes the dependency from “本を (the book)” to “見た (saw)” as depicted by the solid line in Figure 1, occurs with the bi-nominal approaches. This is because the bi-nominal model cannot consider hierarchical structures. Thus, it is impossible to perform accurate parsing for a statement that has a complex structure.

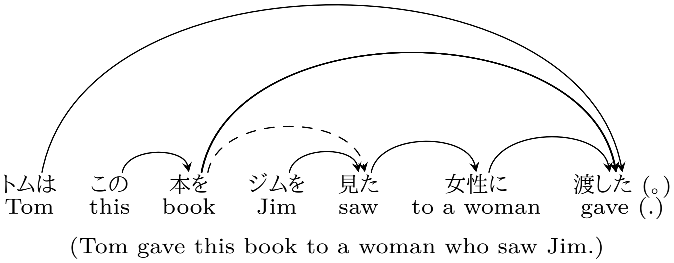


Figure 1. Example of parsing in Japanese language

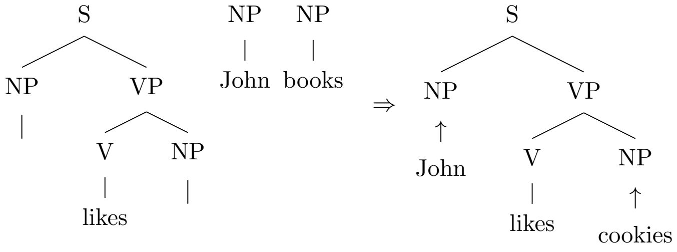
Therefore, we propose a new method for dependency parsing in Japanese language that uses the hierarchical structure relation of phrases.

B. Tree Substitution Grammar

Tree Substitution Grammar (TSG) is an extension of Context Free Grammar (CFG) [5]. Both CFG and TSG have rewrite rules, called productions, which are used to construct syntax trees by replacing nonterminal symbols with elementary trees which is a part of the syntax tree.

The TSG production replaces a nonterminal symbol with an elementary tree whose depth is greater than one while the CFG production does the same with an elementary tree whose depth is exactly one. As a result, the TSG production has a hierarchical structure based on any context. TSG is 4-tuple and is defined as $G = \{T, N, S, R\}$, where T is a set of terminal symbols, N is a set of nonterminal symbols, $S(\in N)$ is a set of the distinguished root nonterminals, and R is a set of productions. In general, the syntax tree of an English sentence is described as a tree structure because of its phrase-structure rule.

Here, the root node is labeled with a nonterminal symbol, and its leaf nodes are labeled with either terminal symbols or nonterminal symbols. In short, the syntax tree of the input sentence is constructed by recursively replacing the nonterminal symbols with the elementary trees.



Upper arrow “↑” indicate substitution sites in TSG.

Figure 2. A syntax tree comprising three elementary trees

Figure 2 shows an example of parsing from the syntax tree, which is labeled on the left. For example, the S → (NP (VP (V like) NP)) production rewrites the nonterminal symbol S with the fragment (S NP (VP (V likes) NP)). This syntax tree has two NPs as its nonterminal symbols, and the production rewrites these nonterminal symbols with the fragments (NP John) and (NP cookies). In short, a derivation creates a tree by starting with the root symbol and rewriting (substituting) it with an elementary tree, then continuing to rewrite frontier nonterminals with elementary trees until there are no remaining nonterminals.

In TSG, the replacement of nonterminal symbols with elementary trees is performed in an arbitrary manner; however, we can calculate the probabilities of the rewriting rules in the syntax tree. Probabilistic Tree Substitution Grammar (PTSG) is an extension of TSG whose productions have their probabilities $P(e|c)$ where the elementary tree e replaces a nonterminal symbol c.. $P(e|c)$ is statistically calculated on the basis of training data. The distribution of the PTSG production G_c can be generated by the Hierarchical Pitman-Yor process [8] as follows:

$$G_c \sim \text{PY}(d_c, \theta_c, G_{\pi(c)}) \qquad (5)$$

where d_c and θ_c are hyper-parameters in the Hierarchical Pitman-Yor process when we give the nonterminal symbol c, and $G_{\pi(c)}$ is a distribution over the infinite dimensional distribution of the elementary tree with c.. To generate e, we now draw e_1 from G_ϕ giving us an elementary tree with nonterminal symbol $c_1, \ldots, c_m$, and then draw $e_2, \ldots, e_m$ in turn from base measure $G_{\pi(c_1)}, \ldots, G_{\pi(c_m)}$. We continue in this fashion until a full tree is generated.

However, a problem associated with the segmentation of elementary trees arises when PTSG is derived. Gibbs sampling, in which random variables are repeatedly sampled conditioned on the current values of all other random variables in the model is usually used to solve this problem. Figure 3 shows an example of segmentation of a syntax tree.

In the procedures described above, we can perform dependency parsing based on hierarchical structure. This method, the state-of-the-art in English dependency parsing [6], is known as Symbol Refined TSG (SR-TSG). SR-TSG applies *symbol refinement* techniques [11], [12] to parse English sentences. These techniques are used in parsing methods that have no hierarchical structure, such as CFG. Thus, although not directly related to TSG, the symbol refined syntax trees constructed by SR-TSG use a state-of-the-art method.

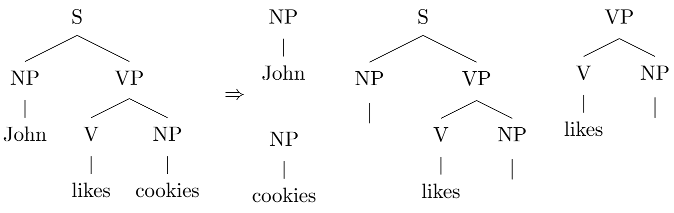


Figure 3. Elementary trees based on PTSG

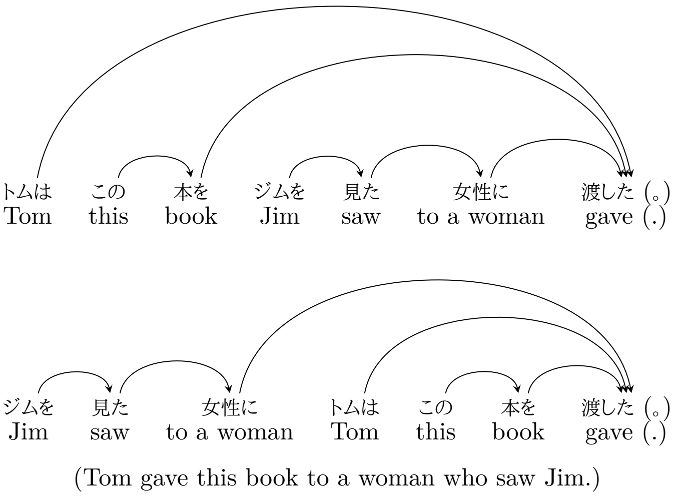


Figure 4. Two Japanese sentences that have the same structure

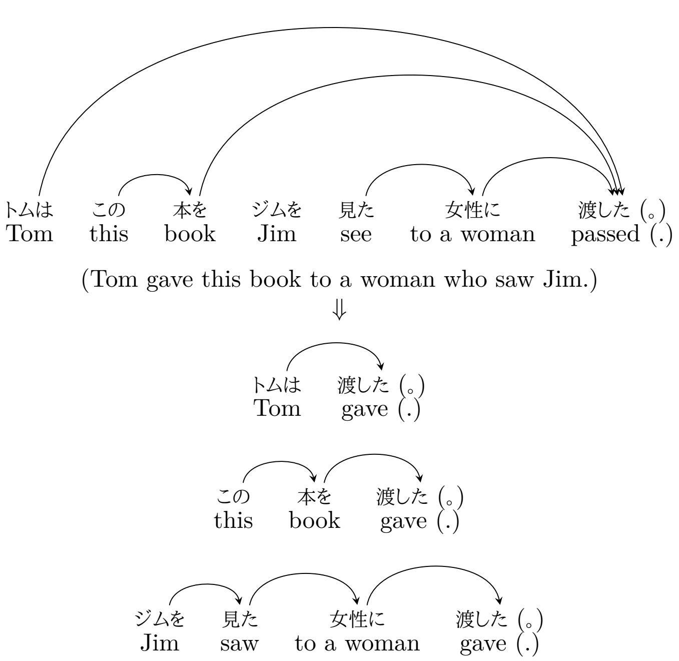


Figure 5. Hierarchical dependencies in the Japanese language

However, TSG cannot support dependency parsing in Japanese language because its syntax tree cannot have a tree structure as postpositions in the Japanese language represent the syntactic function of each phrase. For example, there are two sentences in Figure 4. The phrase order is different in the two sentences, while each phrase has the same dependencies. Therefore, it is impossible to conduct dependency in Japanese language parsing in TSG which is applied to the language syntax tree to express it as a tree structure. As a result, we propose a novel dependency parsing method in Japanese language that considers both the weak context dependency and the order of phrases using an extension of TSG.

IV. Hierarchical Dependency Parsing

In this section, we propose a method in Japanese language for parsing dependencies with weak contexts.

A. Syntax Tree Construction

In order to consider dependencies between phrases, we generate a syntax tree based on the n-gram model made from the occurrence of dependencies. We can calculate the probabilities of the referrer phrases subject to occurrence of the destruction phrase. For example, in the dependency between phrase "トムは"(Tom) and "渡した"(gave) referrer phrase "トムは"(Tom) depends on the referenced phrase "渡した"(gave). Then, occurrence probability of the dependency between phrase "トムは"(Tom) and "渡した"(gave) is calculated as the conditional probability $P_D(\text{トムは} \mid \text{渡した})P_D(\text{Tom}|\text{gave})$ that is the bi-gram model used as a prior probability $P_D(\text{渡した})(P_D(\text{gave}))$.

At present, we cannot construct an n-gram model that reflects the occurrence of phrases if n is small. Conversely, the size of the n-gram model is large if n is large.

In order to solve this problem, we use Variable-order Pitman-Yor Language Model (VPYLM) [13], an extension of the hierarchical Pitman-Yor process [8]. This technique can help to treat n as as any variable in the n-gram model. Using VPYLM, we can generate a syntax tree model considering the number of phrases when we calculate the probabilities of the referrer phrase as being the root node of the elementary tree. For example, Figure 5 shows three elementary trees comprising the end of a sentence. In short, we can get three hierarchical dependency trees and can calculate the probabilities $P_D(\cdot| \text{渡した})$ of the end of a sentence being the root node. Thus, we can generate a precise syntax tree with weak context dependency.

B. Hierarchical Dependency Parsing Algorithm

Dependencies in Japanese language have the following limitations:

- Japanese is a head-final language. Except for the rightmost one, thus, each segment modifies exactly one segment among the segments appearing to its right.
- Dependencies do not cross one another.

Since the syntax trees constructed by the method described in Figure 6 (a), each of whose root node is the phrase at the end of the sentence, are hierarchical, we parse the sentence in bottom-up fashion using an algorithm called CYK [14] which is based on depth-first search. The phrase at the end of a sentence gets the dependency from the one immediately before it, so we regard the phrase at the end of the sentence and the one immediately before it as the weak context dependency and find another dependency in the sentence.

In Figure 6 (b), for example, the phrase “渡した” is the phrase at the end of the sentence, so that we can get the dependency from “女性に”. As a result, we can calculate the probability in the calculated probability of the dependency $P_D(\text{女性に} \mid \text{渡した})(P_D(\text{to an woman}|\text{gave}))$. In the same fashion, we can calculate different probabilities of dependencies $P_D(\text{見た} \mid \text{女性に渡した})(P_D(\text{saw}|\text{gave to an woman}))$ and $P_D(\text{見た} \mid \text{渡した})(P_D(\text{saw}|\text{gave}))$, if we assume that there is a dependency between “女性に” and “渡した”. Presently, we compare $P_D(\text{見た} \mid \text{女性に渡した})(P_D(\text{saw}|\text{gave to an woman}))$ with $P_D(\text{見た} \mid \text{渡した})(P_D(\text{saw}|\text{gave}))$, and then, extract the dependency between the phrases. If $P_D(\text{見た} \mid \text{女性に渡した})(P_D(\text{saw}|\text{gave to an woman}))$ is large compared with $P_D(\text{見た} \mid \text{渡した})P_D(\text{saw}|\text{gave})$, we decide that there is a dependency between “見た” and “女性に渡した”. These processes continue to work until we get to the phrase at the beginning of the sentence. In the end, everything for which the relationships are adjudged to be dependencies form the syntax tree of the sentence.

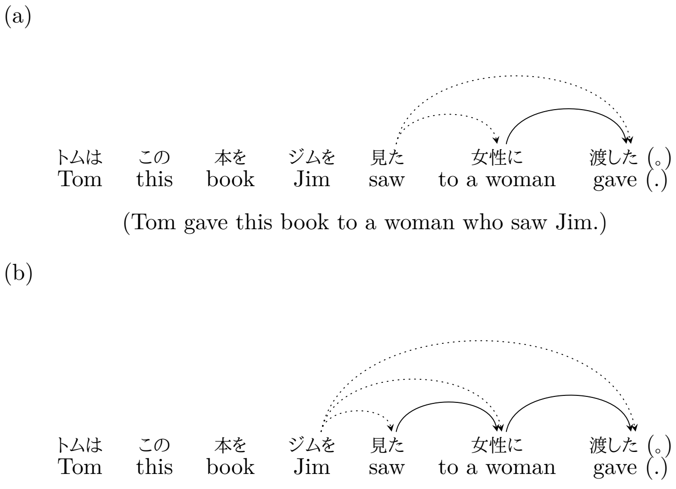


Figure 6. An example of dependency parsing processes using the hierarchical dependency model in Japanese language

V. Experimental Evaluation

To evaluate our method which considers hierarchical structure in Japanese language, we compared it with a conventional one using the Kyoto University Text Corpus [15]. The Kyoto University Text Corpus is a Japanese text corpus for handling the dependencies of morpheme and segment in Japanese language, and is commonly used to evaluate the effectiveness of Japanese language morphological analysis and dependency parsing in Japanese language. We chose CaboCha [1] as the conventional method, because it is said that CaboCha is the most effective method for parsing dependencies in Japanese language. CaboCha itself also used the Kyoto University Text Corpus for its evaluation.

As stated in Section IV, our method utilizes training data to generate syntax trees and parses dependencies in Japanese language using CaboCha and our method; therefore, we calculated the accuracies of dependencies parsed by our method.

A. Experimental Procedures

Although the Kyoto University Text Corpus comprises newspaper articles for five days, we utilized only one day's articles (1100 sentences) of dependencies parsed in Japanese language by our method. This is because it takes more time to get our syntax trees, so that we have to save the processing time.

In our procedure, generating syntax trees, we extract dependencies in Japanese language between phrases, next, construct syntax trees focusing on the phrases at the end of sentences that are assigned to the root nodes of the syntax trees. We then apply the hierarchical Pitman-Yor process and estimate parameters θ using the Gibbs iteration.

Finally, we can obtain dependencies in Japanese language using our extracted syntax tree model. In this procedure, we first divide the sentences into segments after performing Japanese language morphological analysis, and check the segment sequences against our syntax trees. This procedure helps to parse dependencies in Japanese language while continuing to extract the dependencies between phrases from the phrase at the end of an input sentence.

B. Experimental Results

We also performed the same processes using CaboCha based on bi-nominal models [1]. To compare our method with CaboCha, we utilized the following measurement denoted by R that is frequently used to evaluate the accuracies of dependencies:

$$R = \frac{Y}{X} \tag{6}$$

where X denotes the number of dependencies in the test data, and Y denotes the number of dependencies extracted by each parser (our method and CaboCha). Of course, dependencies extracted by the each parser are contained in the test data, so that R is usually termed recall in the information retrieval research field [16]. In order to calculate R using each parser, we randomly selected 200 sentences from newspaper articles from other days that were not used to construct syntax trees. That is to say, we focused on the efficacy of the dependencies extracted by each method. Table I indicates that our method is, unfortunately, inferior to CaboCha from the viewpoint of effectiveness. This is because our method utilizes syntax trees not only using a small quantity features for parsing dependencies in Japanese language. For which, CaboCha parses dependencies in Japanese language with various features (word, lexical form of word, POS tag, and inflectional form), so that the accuracies of parsing dependencies in Japanese language are effective using CaboCha. Therefore, the precision of our method may be improved still more.

TABLE I. Experimental results 1

	CaboCha	our method
R	0.871	0.769

However, our method is ideal for accurately extracting dependencies in Japanese language in long sentences whose

TABLE II. EXPERIMENTAL RESULTS 2

	Our method	CaboCha
complex and long sentences	0.700	0.550

syntax tree has a complex structure. That is, we also have to evaluate sentences from which CaboCha cannot extract dependencies in Japanese language. Therefore, we randomly selected 20 long sentences (10 percent of the test data in previous experiment) with relatively complex structures.

Table II shows that our method was able to extract dependencies accurately from 14 out of the 20 sentences while CaboCha was only able to do this for eleven. In short, our method was better able to parse dependencies in Japanese language from the long and complex sentences than CaboCha. The reason for this is that it is still possible for the parser to interpret the meaning of the postposition in some cases, even if the syntax tree model does not have a hierarchical structure. However, the syntax trees constructed by our method contain not only the relationships between phrases but also the hierarchical structure of each phrase. Consequently, our method can restrain failed analysis of the complex Japanese sentence in by conventionally method.

VI. CONCLUSION

In this paper, we proposed a method for parsing dependencies in Japanese language using novel syntax trees based hierarchical structure, that are constructed by analyzing the relationships between segment sequences. By considering the relationships between segment sequences, our method was able to solve a phrase order problem. In the near future, we plan to utilize not only the order of words but also the result of syntactic and case structure analysis to improve the accuracies of dependencies in Japanese language. We also plan to conduct experimental evaluations using all the data in the Kyoto University Text Corpus.

ACKNOWLEDGMENT

We would like to give special thanks to all who commented on this work at the IPSJ Kansai Workshop 2013 for their assistance in identifying the weaknesses in our work and also for giving suggestions on how to improve it. This work was partly supported by a Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (KAKENHI), Grant Number 25540150.

REFERENCES

[1] T. Kudo and Y. Matsumoto, “Japanese Dependency Analysis using Cascaded Chunking,” in Proceedings of Conference on Natural Language Learning, 2002, pp. 63–69.

[2] Y. Cheng, M. Asahara, and Y. Matsumoto, “Machine learning-based dependency analyzer for chinese,” Journal of Chinese Language and Computing, vol. 15, no. 1, 2005, pp. 13–24.

[3] M. Sassano, “Linear-time dependency analysis for japanese,” in Association for Computational Linguistics, 2004.

[4] M. Post and D. Gildea, “Weight pushing and binarization for fixed-grammar parsing,” in Proceedings of the 11th International Conference on Parsing Technologies, 2009, pp. 89–98.

[5] P. Blunsom and T. Cohn, “Unsupervised induction of tree substitution grammars for dependency parsing,” in Proceedings of Conference on Empirical Methods in Natural Language Processing, 2010, pp. 1204–1213.

[6] H. Shindo, Y. Miyao, A. Fujino, and M. Nagata, “Statistical Parsing with Probabilistic Symbol-Refined Tree Substitution Grammars,” in Proceedings of International Joint Conference on Artificial Intelligence, 2013, pp. 3082–2086.

[7] J. Pitman and M. Yor, “The Two-Parameter Poisson-Dirichlet Distribution Derived from a Stable Subordinator,” The Annals of Probability, vol. 25, no. 2, 1997, pp. 855–900.

[8] Y. W. Teh, “A hierarchical Bayesian language model based on Pitman-Yor processes,” in Proceedings of Association for Computational Linguistics, 2006, pp. 985–992.

[9] H. Ishwaran and L. F. James, “Generalized weighted Chinese restaurant processes for species sampling mixture models,” Statistica Sinica, vol. 13, 2003, pp. 1211–1235.

[10] R. Kneser and H. Ney, “Improved backing-off for M-gram language modeling,” in Proceedings of International Conference on Acoustics, Speech, and Signal Processing, 1995, pp. 181–184.

[11] M. Collins, “Head-Driven Statistical Models for Natural Language Parsing,” Association for Computational Linguistics, vol. 29, no. 4, 2003.

[12] T. Matsuzaki, Y. Miyao, and J. Tsujii, “Probabilistic CFG with Latent Annotations,” in Proceedings of Association for Computational Linguistics, 2005, pp. 75–82.

[13] D. Mochihashi and E. Sumita, “The infinite markov model,” in Proceedings of Annual Conference on Neural Information Processing Systems, 2007, pp. 1017–1024.

[14] N. Chomsky, “Three models for the description of language,” IRE Transactions on Information Theory IT-2, vol. 2, no. 3, 1956, pp. 113–124.

[15] S. Kurohashi and M. Nagao, “Building a Japanese Parsed Corpus while Improving the Parsing System,” in Proceedings of Language Resources and Evaluation Conference, pp. 719–724.

[16] R. Baeza-Yates and B. Ribeiro-Neto, Modern Information Retrieval: The Concepts and Technology behind Search (ACM Press Books), 2nd ed. Addison-Wesley Professional, Feb. 2011.

Intrusion Detection Using N-Grams of Object Access Graph Components

Zachary Birnbaum   Andrey Dolgikh   Victor Skormin
Binghamton University,
Binghamton, NY, USA
{zbirnba1, adolgik1, vskormin}@binghamton.edu

Abstract - **Cyber warfare demonstrates an arms race between mutually escalating malware and Intrusion Detection System (IDS) technologies. We put forward a novel process for defining system behavior with the end result being a highly effective IDS. System calls accumulated under normal network operation are converted into graph components, and used as part of the IDS normalcy profile. This paper are as follows: detection of attacks based on the anomalous use of program functionality; reduced window of attack; reduced false positive rate; increased performance in comparison to standard n-gram methods; a graph compression algorithm for efficient processing of system call graphs. The proposed IDS can be used within limited access environments such as industrial or military systems where only approved applications are running and any anomalies are indicative of a cyber attack or malfunction.**

Keywords: security, intrusion detection, behavioral anomaly detection, graph processing

I. Introduction

Modern computer systems, especially those employed in industrial control and automation spheres, usually feature a diverse software stack and unique configuration. This peculiarity was mentioned as the “Diversity hypothesis” in [1]. The diverse environment results in unique computer system operation as seen from the system call level. This can be successfully used to develop a customized behavioral profile tailored to the particular system under consideration. Customized profiling allows an anomaly detection approach to be used. By comparing the previously established profile with the profile of the running system any extracurricular activity within the system in question can be detected and flagged as an anomaly. Hofmeyr et al in [2] shows that intrusions and certain abnormal situations (e.g. lack of disk space or client misconfiguration) trigger anomaly detections. Therefore the detection of anomalous activity may alert a system operator of an intrusion or abnormal system operation.

II. Related Work

A large number of approaches were developed and studied for anomaly based intrusion detection. We will limit our review to system call based Intrusion Detection Systems (IDS).

Forrest et al in [3] offers a simple and effective method based on the n-gram model:

A sequence of n elements of the same type is called n-gram. For example a trigram consists of three elements (w_1, w_2, w_3). The elements can be of any nature such as numbers, words of natural language, or system calls.

The n-gram model operates as follows:

1. The string of elementary observations $S = w_1, w_2, w_3, \dots, w_k$ over the alphabet of possible observations $\sum$ is transformed into a string of n-grams using a sliding window of size n. For example, for $n = 3$ we will get the following string of trigrams:
$$S^3 = (w_1, w_2, w_3), (w_2, w_3, w_4), (w_3, w_4, w_5), \dots, (w_{k-2}, w_{k-1}, w_k)$$
2. Learning phase: observed n-grams S_i^{n} are accumulated into the database D:
$$D = \bigcup_i S_i^{\mathrm{n}}$$
3. Detection phase: each observed n-gram w is tested if it belongs to database D. If $w \notin D$ (w does not belong to D) the anomaly is detected.

Since its introduction, many modifications of the n-gram model have been offered, but with marginal improvement [4, 5, 6]. Recent notable large scale efforts to apply the n-gram model to malware detection were carried out by Lanzi et al in [7]. Lanzi performed large scale data collection covering ten different hosts under normal use over a prolonged period of time and thousands of malware samples. Forrest and Lanzi built their n-gram IDS with an observations alphabet $\sum$ equal to the set of system calls defined by the monitored system. Both models normally result in a high rate of anomaly/malicious n-gram detections. Therefore, some mechanism was needed to separate real attack n-grams from false detection. The Forrest approach uses the fact that an attack usually occurs within a very short time period and generates bursts of anomalous n-grams. To average out false positives and highlight the attacks, gram-to-gram Hamming distance and normalization over the trace length was used. Lanzi used the detection count of malicious n-grams exposed by each program. When the detection count crossed the threshold value an attack was declared. In spite of these techniques both approaches still have a high false positive rate that prevents their successful application in practice. This can be attributed to the inability of n-grams to distinguish long range dependencies from noise.

Methods different in nature from n-gram models use various kinds of additional information to recover and monitor program control or data flow [8, 9, 10, 11, 12].

Our approach exceeds the performance of the simple n-gram model by using recognized data flow graph components as a source alphabet. Graph components capture completed and semantically meaningful sequences of system calls. The use of graph components helps to eliminate the mentioned inability of n-gram models to capture long contexts. Thus our approach combines n-gram and data flow approaches to cover long spans of program operation.

II.1. Our Approach

The principal idea behind our behavior based IDS is the detection of anomalous use of known program functionalities. In other words, the IDS detects non-standard, previously unseen use of known program functions.

In order to establish a behavioral profile of the program our IDS consumes intercepted system calls with their respective parameters similar to Kolbitsch [13] and Mutz [10]. Using this information, we can trace how each OS object is accessed. This access history can be represented by an Object Access Graph (OAG). After a sufficiently long time, the OAG represents the essence of normal system operation. This facilitates structural anomaly detection, i.e. the detection of anomalous graph components not seen before in the system.

To capture the context of different program functionalities or structural components we use n-gram model. At this point anomalies can be detected by comparing the n-grams obtained from the current OAG to n-grams accumulated during the learning stage.

Any OAG component of a running system can be incorporated into the normalcy graph, thus rendering reinforcement of the structural normalcy profile trivial. Moreover, detected anomalous components labeled by a human expert as malicious can be instantly added to the malicious profile and later recognized as malware skipping the last n-gram detection stage.

II.2. Contributions

We report the following contributions:

- Detection of attacks from the anomalous use of program functionality (section 3.8).
- Reduced false positive rate in comparison to standard n-gram methods (section 4.4.a).
- Reduced window of attack (section 4.4.b).
- Increased performance in comparison to standard n-gram methods (section 4.5).

III. System Overview

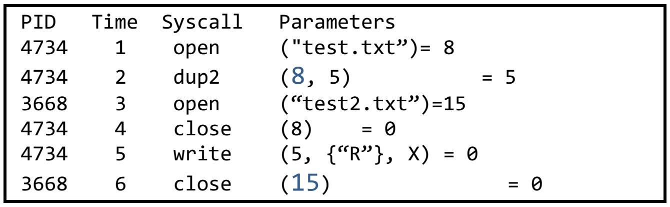
III.1. System Call Monitoring

A number of methods exist to intercept system calls and extract their parameters on the majority of OSs. Kernel driver enabled techniques demonstrate negligible overhead [9, 11]. For convenient research and testing purposes, we chose the Linux kernel and the *strace* system call monitoring program as our platform [14]. The research conducted on this platform is generic and can easily be duplicated on other platforms given they provide similar data.

Linux provides approximately 200 different system calls. *Strace*, a debugging utility, is included in the Linux operating system and is capable of monitoring system calls from all non-system processes [14]. To support a system wide monitoring approach, we use *strace* options that allow us to capture data from processes created after system call monitoring began.

III.2. Data Parsing

Strace output contains very useful information, including the time of the system call, the system call name, and most importantly, the argument values for the system call. The argument values vary depending on the system call, but all relevant information will be listed in the *strace* output. A typical output of *strace*:



```
PID   Time  Syscall   Parameters
4734    1    open      ("test.txt”)= 8
4734    2    dup2      (8, 5)           = 5
3668    3    open      (“test2.txt”)=15
4734    4    close     (8)    = 0
4734    5    write     (5, {“R”}, X) = 0
3668    6    close     (15)              = 0
```

Figure 1. Sample of *strace* output

As seen in the sample of strace output, the process 4734 at time 1 opened the file “test.txt” and has a handle of 8. Any subsequent calls using the same object refer to handle 8 instead of the specific file “test.txt.” This parameter value dependency is a key concept that is crucial to building an Object Access Graph.

III.3. Object Access Graph

Observing system calls with their parameters provides a useful model of system behavior. This model is represented by a vertex-edge, directed, and acyclic graph constructed from the parsed *strace* output and can be described as follows:

$$\boldsymbol{G_m}=(\boldsymbol{V}, \boldsymbol{E}, \boldsymbol{F_v}, \boldsymbol{F_e})$$

where
V – set of vertices,
E – set of edges,
$\boldsymbol{F_v}$ - mapping from ***V*** to set of system calls ***S***.
$\boldsymbol{F_e}$ - mapping from ***E*** to set of system call argument types ***T***.

The graph $\boldsymbol{G_m}$ can be built from the *strace* data according to the following rules:

- Labeled vertex v_s is added to $\boldsymbol{G_m}$ for each issued system call *s*.
- Labeled edge e_τ from v_i to v_j is added for system calls *i* and *j* when one of the parameters of *i* and j have the same data type τ, have equal data value *d*, and have one of the following:
  - v_i has *d* as the output and v_j takes *d* as the input
  - v_i was the last system call registered before v_j

For example, *open* and *dup2* (Figure 1) occur at times 1 and 2, respectively, and have a common parameter of handle type equal to 8. In the resulting graph (Figure 2b), nodes corresponding to calls *open* and *dup2* are connected with the directed edge 8. Nodes *dup2* and *close* are also connected with an edge labeled 8 because the *close* that occurred at time 4 uses the same handle 8.

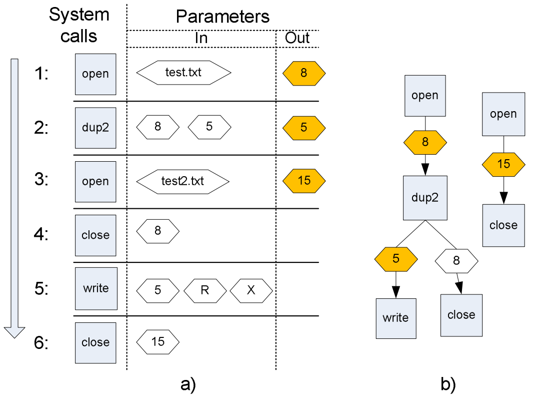


Figure 2. Conversion of system call stream (a) into Object Access Graph (b)

These rules allow us to trace how each OS object is used by different processes. Unlike program centric approaches taken by the majority of Behavior Based IDS [8, 13], this method centers on the system wide behavioral picture imposed by programs over OS objects.

III.4. Graph Component Detection

There are certain terminating system calls defined by the kernel (e.g. *close*, *exit_group*). Once these system calls have been executed over a particular OS object reference, there can be no additional system calls using this reference. In the OAG this means that the component cannot be extended once all its leaves end with terminating calls. Consider the OAG in Figure 3 which contains three completed components.

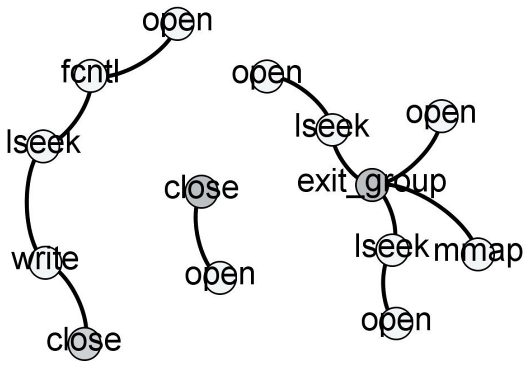


Figure 3. Completed components in OAG

Component detection transforms the stream of system calls into a stream of completed OAG components.

III.5. Component Compression

Due to the repetitive/cyclic actions usually performed by programs over OS objects, some OAG components may grow to unmanageable sizes. However, repetitive occurrences of a single system call or some graph substructures do not provide the observer with substantial additional information. Moreover, it has a detrimental effect on graph recognition.

Consider the graphs featured in Figure 4.a, 4.c. These graph instances represent typical large system call graph components. These graphs are simple in nature but have large node counts that reflect repetitive operations usually performed by programs over one or two OS objects. For example, a network input-output routine may repeatedly send data in small chunks, generating long chains of sends/receives over the socket handle. This type of behavior impairs the recognition process in two ways: First, large graphs take a lot of computing resources to process them. Second, the number of substructure repetitions and consequently the graph component size may depend on factors irrelevant to exposed behavior. This in turn leads to unnecessary component duplication in the database of known components. Therefore it is beneficial to remove/collapse repetitive subgraphs as shown in Figure 4.b, 4.d. It reduces processing load and substantially decreases the number of different graphs observed throughout program operation.

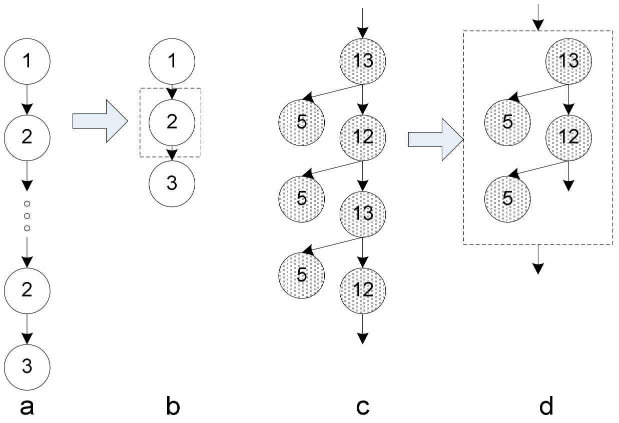


Figure 4. Graph compression

We perform frequent subgraph compression in two stages: First we remove long repetitive chains of single call as show in Figure 4 (a, b). Second, we apply the modified Graphitour algorithm [15] to find and remove/collapse more complex repetitive components.

III.6. Graph Component Database

After compression every completed graph component *c* is subjected to the following normalcy profiling algorithm:

```
Input: completed component c,
       set of components DB={d1, d2, …}
Output: Component database DB
----------------------------
Begin
  foreach $d \in DB = \{d_1, d_2, \dots d_n\}$ do
     if $IsIsomorphic(c, d)$ then continue
     else $Db = Db \cup c$
End
```

Figure 5. Normalcy profiling algorithm

Where the function *IsIsomorphic* tests if two graphs have the same structure.

The algorithm produces a compact database containing one instance of each observed graph component. Using this database, we can detect components that have not been previously encountered. Therefore, it constitutes a normalcy profile of the system.

III.7. Anomalous Component Detection

Once malware has been introduced to the system, it will perform its mission, resulting in additional system calls. Malware functionality will differ from normal system operation and new, unknown OAG components will be observable.

```
Input: completed component c,
       set of components DB={d1, d2, …}
Output: Match or No_match
----------------------------
Begin
  foreach $d \in DB = \{d_1, d_2, \dots d_n\}$ do
     if $IsIsomorphic(c, d)$ then return Match
  return No_match
End
```

Figure 6. Anomaly detection algorithm

These new components, along with components consistent with standard operation, are fed to the anomaly detection algorithm. The anomaly detection algorithm is similar to the profiling algorithm in Figure 5. However, it returns No_match instead of updating the database, when an unknown component is detected.

At this point, we are able to detect the manifestation of malware intrusion in the domain of system call graph components. Using this approach, malware becomes discernible system-wide at a higher semantic level.

III.8. N-grams applied to graph components

To detect the anomalous use of known program functionalities identified by the algorithm in Figure 6 we apply the n-gram model. The model operates as follows:

```
1. The string of system call observations
   $S = w_1, w_2, w_3, \dots, w_k$ is converted into string of
   graph components $S' = c_1, c_2, c_3, \dots, c_k$ using algorithm
   featured in section 3.3.
2. Sliding window is used to convert string of
   observed graph components into string of
   graph-n-grams:
   $S'^n = (c_1, \dots, c_n), (c_2, \dots, c_{n+1}), \dots, (c_{k-n-1}, \dots, c_k)$.
3. Learning phase: graph-n-grams are accumulated
   into database
   $$D = \bigcup_i S'^n_i$$
4. Detection phase: each observed graph-n-gram is
   tested if it belongs to accumulated database.
   All graph-n-grams that are not present in
   normalcy database are detected as anomalous.
```

Figure 7. Learning algorithm for n-gram components over graphs

N-grams over OAG components capture system behavior at the level of program functional blocks such as complete network IO or file editing. This allows us to detect tampering with program control flow at a higher semantic level.

IV. Experimental Evaluation

In this section we provide experimental evaluation for each step of the detection pipeline. The experimental data is available to the public [22].

IV.1. Experimental Setup

In order to evaluate the IDS, we utilized the experiment featuring three computers connected to a common network: victim computer, attack computer, and IDS computer. The victim computer represents the Metasploitable Virtual Machine [16]. The Metasploitable Virtual Machine is an OS package, preconfigured with many exploitable services. In our experiments, we used FTP server (vsFTPd 2.3.4), Samba service (version 3.0.20-Debian), and HTTP Apache server (version 2.2.8) with PHP (version 5.2.12) installed. The victim computer was running a customized *strace* program, which forwarded the system call stream to IDS computer.

The attacking computer is represented by Backtrack Linux, packaged with the Metasploit framework. Metasploit is a software package which comes with tools for vulnerability scanning and penetration testing [17]. Using Metasploit on the attacking computer, we mounted an exploit against services on the victim machine.

A third computer acts as our Intrusion Detection System. The IDS assembles system calls sent from the monitored victim into OAG components. It then passes components into the anomaly detector. At the same time, all activity at the victim host is visualized for expert analysis.

IV.2. Component Database Stabilization

To confirm that our IDS is capable of extracting a limited size OAG component database by processing a volume of system calls data, we ran several tests with loads of different natures: no load, FTP load, HTTP/PHP load, and Samba load. We exercised the FTP server with two different FTP clients by repeatedly connecting/disconnecting, copying small and large volumes of data, changing file permissions, etc. The same approach was taken with the Samba server. The HTTP/PHP server was tested by manual browsing through the sample web site. The results are presented in Figure 8, where the Y-axis illustrates the total number of components in the OAG component database profile, and the X-axis represents the system runtime in number of system calls. With time, all four graphs quickly flatten out, showing that the normalcy profile converges to certain size, which represents all functionality exercised by system.

For each type of load, the absolute number of learned graph components, its average, and maximum sizes stored within the profile are presented in Table 1.

TABLE 1. NORMALCY PROFILE METRICS

	No Load	Samba	FTP	HTTP/ PHP	Combined Profile
Largest Component	10	8	8	12	12
Number of System Calls	94556	575800	483458	107086	1260900
Number of Nodes in Components	55	42	57	83	130
Number of Components	13	11	15	17	26

A useful feature of our IDS approach is the ability to combine different normalcy profiles into one normalcy profile. The combined profile can be used to recognize behaviors from each incorporated profile. By its nature, the combined profile cannot contain duplicate components, therefore keeping only one copy of each. One may assume that components from the no load profile must be present in all subsequent profiles as a background. This is not entirely correct as background operations performed by various daemons are time dependent. Therefore, certain operations observed in the no load profile are not present in Samba profile as we run Samba profiling at a different time. The combined profile automatically takes care of such issues.

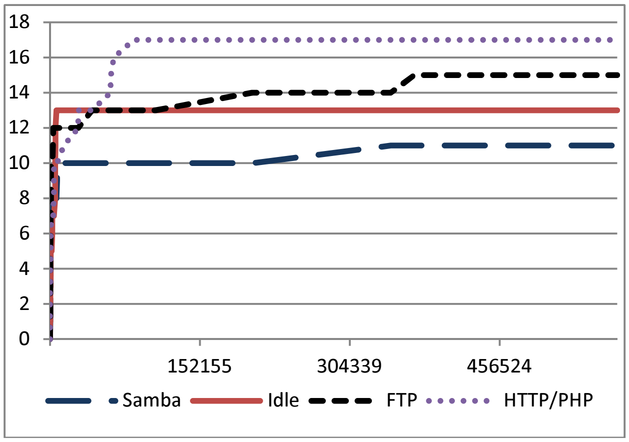


Figure 8. Stabilization of the graph component database size.

IV.3. N-gram Database Stabilization

The next step is to confirm that the database of n-grams learned from the stream of OAG components according to algorithm in Figure 7 converges to a limited size. Figure 9 shows that the database converges for both direct system call n-grams and OAG n-grams. This stabilization was observed under various loads: Idle, Samba, HTTP/PHP, and FTP.

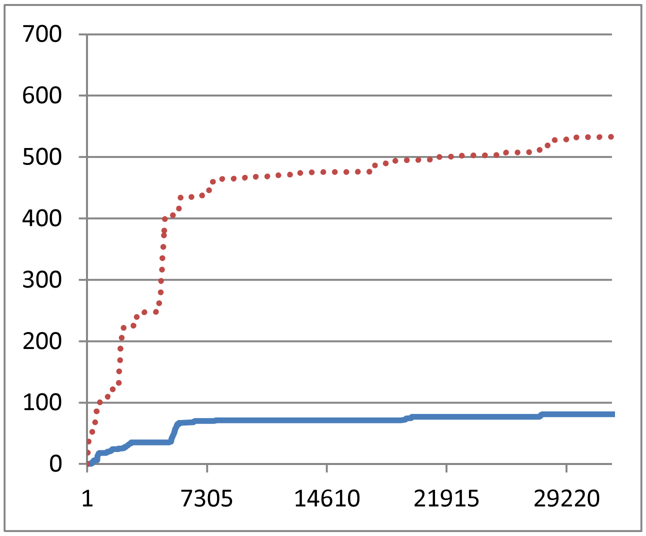


Figure 9. Stabilization of component 3-grams (solid line) and system call 3-grams (dotted line) under no load

One may notice that OAG n-gram database has much lower n-gram counts in comparison to direct system call n-grams. We attribute this to the ability of our system to capture logically finished sequences of program actions.

TABLE 2. COMPARISON OF N-GRAM PROFILE DATA

	# Syscalls	n	OAG n-gram DB size	direct n-grams DB size
No Load	94556	3	91	628
		5	194	1159
		10	390	2510
Samba	575800	3	67	449
		5	125	858
		10	384	2398
FTP	483458	3	182	2808
		5	467	9775
		10	1111	36005
HTTP/ PHP	107086	3	126	1222
		5	263	2517
		10	558	4767

The pitfall of direct n-grams is a small viewing window. As a result, events connected over a longer period are viewed by system as anomalies. The OAG-based system has much wider context awareness. As a result, it makes fewer errors and requires fewer n-grams to achieve similar or better performance. As seen in Table 2, longer n-grams require larger databases to cover the same activity. Regardless of n, the OAG approach requires a significantly smaller database to capture program normal behavior.

IV.4. Anomaly Detection

In this section, we discuss the detection capability of the anomaly detection algorithm under three types of loads: file and print services (Samba), web services (HTTP/PHP), and file transferring services (FTP).

Metasploitable, serving as our victim machine, is prepackaged with vulnerable services (see Table 3).

All experiments were performed in real time according to the procedure featured in Figure 10. For all tests the n-gram normalcy profile is represented by a merged normal behavior for all loads.

```
0. Start the IDS machine and load n-gram database.
1. Start victim host.
2. Enable system call tracing on the victim host.
3. Start vulnerable service on the victim host.
4. Exercise the service with a normal load.
5. Launch the attack against vulnerable server.
6. Observe detected anomalous n-grams.
```

Figure 10. Experiment procedure

In the experiments, we demonstrated the ability of OAG n-gram and direct n-gram approaches to successfully detect anomalies induced by exploitation attacks. Table 4 summarizes empirical data obtained in the experiments.

Both approaches register anomalies induced by performed attacks. Our OAG n-gram method matches the detection performance of the direct n-gram approach.

TABLE 3. EXPERIMENTAL SETUP

Version	Samba	3.020-Debian
	HTTP/PHP	Apache 2.2.8/ 5.2.12
	FTP	vsFTPd 2.3.4
Exploit	Samba	*/multi/samba/usermap_script*
	HTTP/PHP	*/multi/http/php_cgi_arg_injection*
	FTP	*/unix/ftp/vsftpd_234_backdoor*
Normal activity test	Samba	upload, download, delete, and create files and folders
	HTTP/PHP	browsing hosted pages
	FTP	upload, download, delete, and create files and folders

Increasing values of n results in a greater number of anomalous grams detected. Therefore larger values of n are beneficial for increased sensitivity to attacks. Regardless of the gram size OAG approach shows lower anomaly counts. This is due to the OAG approach operating on a higher semantic level (graph component level) than direct n-grams (system call level).

TABLE 4. ANOMALY DETECTION

		Anomalies	
	n	direct n-gram	OAG n-gram
FTP	3	182	27
	5	552	99
	10	1376	252
SAMBA	3	211	24
	5	509	81
	10	1028	261
HTTP/ PHP	3	54	3
	5	136	51
	10	341	82

IV.4.1. False Positive Rate

To measure the false positive rate we repeated the experimental procedure featured in Figure 10 however no attack was launched (no step 5). The results of the experiments are summarized in Table 5.

TABLE 5. FALSE POSITIVE RATE

		False positives	
	n	direct n-gram	OAG n-gram
FTP	3	144	6
	5	319	22
	10	668	60
SAMBA	3	1065	12
	5	2374	41
	10	4520	92
HTTP/PHP	3	49	3
	5	292	16
	10	467	47

The OAG approach produces fewer false positives than the direct n-gram approach across all services.

IV.4.2. False Negative Rate

Wagner and Dean proposed a statistical mimicry attack against n-gram based methods [18]. We significantly reduce the window of opportunity for such attacks. Now the attacker would need to mimic n-gram statistics, OAG components and OAG n-gram statistics to successfully evade detection. Wagner's method relies on generating long lists of dummy system calls. These dummy system call sequences applied randomly will not match the OAG profile. Therefore proper implementation of Wanger's attack under OAG will require generation of system call sequences that match the OAG profile. This means the attacker cannot sneak in any new functionality and is forced to use functional components already present in the system normalcy profile.

IV.5. Performance Evaluation

We present the runtime performance of our IDS in two dimensions: capturing overhead and detection overhead.

Capturing overhead measures the performance penalty incurred by *strace*. Tests performed using Samba, FTP, and PHP with *strace* enabled did not show noticeable slowdown. A synthetic test using a custom program designed to stress system call interface showed a tenfold runtime increase. The capturing overhead is dependent upon the mechanism used. For example, a kernel driver implementation will result in negligible overhead ([9] reports less than 6% overhead).

TABLE 6. DETECTION OVERHEAD

		Trace Length		Time Spend Detecting	
	n	system calls	OAG components	Direct	OAG
FTP	3	11971	346	0.26	0.29
	5	11971	346	1.006	0.29
	10	11971	346	5.25	0.29
Samba	3	55163	341	9.25	0.35
	5	55163	341	34.29	0.37
	10	55163	341	128	0.36
HTTP/ PHP	3	9503	586	0.36	0.53
	5	9503	586	2.62	0.56
	10	9503	586	15.55	0.53

Detection overhead measures the anomaly detector performance's impact on system operation. For OAG based approach it includes reduction of raw data into graph components and graph gram matching. Table 6 shows that OAG n-gram matching approach is extremely efficient, resulting lower overhead when compared to the direct n-gram method with larger n. As n increases, the OAG approach doesn't slow down unlike the direct method. This can be attributed to a much smaller database of OAG n-grams.

V. LIMITATIONS

Our approach assumes a tamper-free data source. We do not have the ability to detect attacks completely hidden by rootkits [19]. However if a rootkit is used to hide only a certain subset of system calls it is likely to break the dependence of calls within OAG components or OAG n-grams thus revealing itself as an anomaly. The same is true for attacks relying on race conditions [20].

Attacks that do not change the program control flow (such as [21]) are not detected by our IDS. However, several important cases of such attacks are still detectable. For example, when the attack alters the data flow, it results in changes of the OAG.

Attacks that make use of misconfigured resources in a legitimate way may not be detected if the same functionality is routine.

Our approach for system normalcy relies on past system behavior. Any unidentifiable future behavior, benign or malicious, as previously discussed, will trigger an anomaly.

VI. CONCLUSION

The widespread use of malicious software continues to be an ever-growing concern. Our research resulted in a prototype IDS built on two key ideas: The transformation of system calls into graph components and matching their sequences.

The IDS employs several novel concepts for program data flow processing. We establish an Object Access Graph (OAG) representing interdependent program operations over OS objects. The OAG is compressed to efficiently represent the essence of program activity. OAG components are subjected to a well known n-gram method.

The developed IDS yielded promising results in several aspects. First, the IDS can detect attacks disguised as normal system operation by using existing program functionality. Second, our method significantly reduces the attack window by monitoring program behavior at different semantic levels.

Experiments demonstrated both a reduction in the false positive rate as well as increased performance when compared to standard n-gram methods. Results also showed that the IDS is capable of detecting unknown attacks against system services.

Our results show that achieving efficient anomaly detection is possible through the intelligent application of graph processing algorithms to system behavioral profiling.

ACKNOWLEDGMENTS

This research is funded by the Air Force Office of Scientific Research (AFOSR) project FA9550-12-1-0077. The authors are grateful to Dr. Robert Herklotz for supporting this effort.

References

[1] S. Forrest, S. Hofmeyr, A. Somayaji, "The Evolution of System-Call Monitoring," Proceedings of the 2008 Annual Computer Security Applications Conference, 2008

[2] S. Hofmeyr, S. Forrest, A. Somayaji, "Intrusion detection using sequences of system calls," Journal in Computer Security. 6, pp. 151-180, 1998

[3] S. Forrest, S. Hofmeyr, A. Somayaji, T. Longstaff, "A sense of self for Unix processes, "Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on , vol., no., pp. 120-128, 6-8 May 1996

[4] C. Warrender, S. Forrest; B. Pearlmutter, "Detecting intrusions using system calls: alternative data models," Security and Privacy, 1999. Proceedings of the 1999 IEEE Symposium on , vol., no., pp.133-145, 1999

[5] A. B. Somayaji, "Operating System Stability and Security Through Process Homeostasis," Ph.D. Dissertation. The University of New Mexico. 2002

[6] N. Hubballi, S. Biswas, S. Nandi, "Sequencegram: n-gram modeling of system calls for program based anomaly detection," Communication Systems and Networks (COMSNETS), 2011 Third International Conference on , vol., no., pp.1-10, 4-8 Jan. 2011

[7] A. Lanzi, D. Balzarotti, C. Kruegel, M. Christodorescu, E. Kirda, "Access Miner: using system-centric models for malware protection," Proceedings of the 17th ACM conference on Computer and communications security, pp. 399-412, 2010

[8] R. Sekar, M. Bendre, P. Bollineni, D. Dhurjati, "A fast automaton-based approach for detecting anomalous program behaviors," IEEE Symposium on Security and Privacy, pp. 141, 2001

[9] D. Gao, M. Reiter, D. Song, "Gray-box extraction of execution graphs for anomaly detection," Proceedings of the 11th ACM conference on Computer and communications security, pp. 318-329, 2004

[10] D. Mutz, F. Valeur, G. Vigna, C. Kruegel, "Anomalous system call detection," ACM Trans. Inf. Syst. Secur. 9, 1, pp. 61-93, 2006

[11] A. Tokhtabayev, V. Skormin and A. Dolgikh, "Expressive, Efficient and Obfuscation Resilient Behavior Based IDS," Proc. European Symposium on Research in Computer Security, pp. 698-715, 2010

[12] V. Zwanger, F. Freiling, "Kernel mode API spectroscopy for incident response and digital forensics," In Proceedings of the 2nd ACM SIGPLAN Program Protection and Reverse Engineering Workshop, article 3, 2013

[13] C. Kolbitsch, P. Comparetti, C. Kruegel, E. Kirda, X. Zhou, X.Feng Wang, "Effective and efficient malware detection at the end host," Proceedings of the 18th conference on USENIX security symposium, pp. 351-366, 2009

[14] Online. strace software, http://linux.die.net/man/1/strace, retrieved Feb 2013

[15] L. Peshkin, "Structure induction by lossless graph compression," In Proceedings of the 2007 Data Compression Conference (DCC '07, pp. 53-62, 2007

[16] Online. Metasploitable Virtual Machine, https://community.rapid7.com/docs/DOC-1875, retrieved Feb 2013

[17] Online. Metasploit Software, http://www.metasploit.com/, retrieved Feb 2013

[18] D. Wagner, D. Dean, "Intrusion Detection via Static Analysis," In Proceedings of the 2001 IEEE Symposium on Security and Privacy, pp. 156, (SP '01)

[19] A. Srivastava, A. Lanzi, J. Giffin, D. Balzarotti, "Operating system interface obfuscation and the revealing of hidden operations," Proceedings of the 8th international conference on Detection of intrusions and malware, and vulnerability assessment, pp. 214-233, 2011

[20] R. Watson, "Exploiting concurrency vulnerabilities in system call wrappers," Proceedings of the first USENIX workshop on Offensive Technologies, article 2, 2007

[21] C. Parampalli, R. Sekar, R. Johnson, "A practical mimicry attack against powerful system-call monitors," Proceedings of the 2008 ACM symposium on Information, computer and communications security, pp. 156-167,2008

[22] Online, strace traces, http://testbed.binghamton.edu/traces

Raising Fraud Awareness through Web Forums

Vrizlynn L. L. Thing

Cybercrime & Security Intelligence Department
Institute for Infocomm Research, Singapore
vriz@i2r.a-star.edu.sg

***Abstract*—Topic specific forums, which contain a vast amount of information can aid in providing very useful and informative advice to their readers. Forums that are specific to scam complaints (and reporting) can also aid in raising public awareness to new scams and fraudulent activities, and provide the support for a more pro-active approach to the early detection and prevention of fraud. Accurate and efficient provision of contents from forum sites are therefore very important, to provide information to aid in preventive measures. In this paper, we acquire data from 6 popular and active scam reporting forums with varying ages (from 1.07 to 9.45 years old). We then carry out an analysis to investigate the ability to extract posts detailing victims' encounter with scams and fraud, based on the coverage via simple searches on specific keywords and keyword combinations. We also carry out an evaluation of the merchant coverage in each forum and investigate the association of keywords to support future reliable informative data provision from both topic-specific, and generic forums and online sources.**

***Index Terms*—Fraud detection, fraudulent merchant, fraudulent activity analysis, scam, complaint, forum.**

I. Introduction

The widespread use and contributions of knowledge in the form of data uploaded to the Internet has made it a wealthy source of information for any conceivable topics. One of the most important platforms on the Web is the online forums. Online web forums' dynamically increasing contents, which is contributed by millions of Internet users on a daily basis, has led to its increasing richness of information. Its widespread popularity is its facilitation of global, convenient, fast and freely open discussions. Therefore, web forum data is an accumulation of a vast collection of updated human knowledge and viewpoints. Forums can thus be a highly valuable source of online information for knowledge acquisition to build up domain expertise [1], improve business intelligence [2], [3], [4], and early detection of the presence (and study) of extremist activities [5], [6], [7], [8], [9].

In [5], the authors proposed a framework for Web forum data integration to support the analysis of interactions among discussion participants. The targetted forums were Jihadist forums. The authors introduced features such as forum browsing and searching, multi-lingual translation and social network visualization in their work to support the early detection of extremism activities.

In [7], the authors carried out an analysis of U.S. and Middle Eastern extremist group forums. An affect lexicon based on probabilistic disambiguation technique was proposed to measure the presence of hate and violence related words in the forums' contents. The authors concluded that a strong linear relationship exists between the usages of hate and violence related words in the Middle Eastern extremist group forums.

In [8], the authors evaluated the usage of stylistic and syntactic features for the sentiment classification of English and Arabic contents in Web forums. The authors concluded that the stylistic features and their proposed entropy weighted genetic algorithm (incorporating information-gain heuristic for feature selection) could significantly enhance the sentiment classification.

In [3], the authors conducted an experimental study by asking consumers to gather online information on a specific product topic by accessing Web forums. The authors concluded that consumers who acquired information from online forum discussions reported a greater interest in the selected product topic than those who acquired information from marketer-generated sources.

In [4], the authors proposed a scoring technique to evaluate specific product reviews and to summarize the opinions of the product to the user. The methodology enables the user to save time on reading all the reviews and at the same time, arrive at a generic opinion of a product based on the reviews posted on Web forums.

In [9], the authors proposed incorporating message content similarity and response immediacy to measure the degree of influence between any two users on Web forums. To ensure an accurate approach of measurement, the authors proposed the design of weight application and integration to the typical user link analysis technique. The evaluation of the proposed algorithms was carried out using the ACM Intelligence and Security Informatics KDD challenge to show the potential in identifying influential users.

However, there is no existing work which looks at the analysis of fraudulent and scam related activity reporting forums. Due to the important information they can provide, we think it is necessary to be equipped with an understanding of fraudulent and scam related activity reporting forums. Therefore, in this work, we cover the analysis of fraudulent and scam related activity reporting forums by collecting and analysing a set of popular forums that provide a platform for consumers to report their encounters as victims of scams and frauds. Our work will enable a better understanding of such forums to support the raising of public awareness to new scams and fraudulent activities in the wild, and the early detection of such activities and potential merchants/companies involvement or association.

There are existing works in the area of forum crawling [10], [11], [12], [13], [14] and its content extraction [15], [16], [17], [18], [19]. In this work, we focus on forum content analysis, specifically in scam reporting forums. To the best of our knowledge, this is the first work which carries out an analysis of forum data on fraudulent and scam related activities.

Our main contributions in this paper are:

1) the collection of complete fraudulent and scam related activity reporting posts from active forums ranging from the age of 1.07 to 9.45 years
2) the generation of keywords relevant to fraudulent and scam related activities from the preliminary analysis of online sources of incidents reporting
3) the preparation of the list of companies reported in the scambook forum
4) the analysis of the forums and evaluation of the ability to detect posts detailing fraudulent and scam related activities and events, based on i) our single keyword based analysis, and ii) keyword combination based analysis
5) the evaluation of the merchants (or companies) coverage in each forum, and the investigation of keyword association with each merchant

This work will be valuable in i) providing an in-depth understanding of current popular forum sites related to fraudulent and scam related activity reporting, ii) enabling us to make recommendations based on the findings from this research, and iii) generating top relevant keywords as supporting features to detect merchants and activities related to fraud and scams in both topic-specific and generic online sources.

The rest of the paper is organised as follow. In Section II, we describe our target forums and carry out a preliminary analysis to obtain useful statistics. In Section III, we propose the analysis of the forum post data/content based on our generated keyword list, and present and discuss our results. In Section IV, we extract companies' names from the scambook forum, propose the procedural steps to clean the list to prevent high false positives and false negatives during detection, and analyse the coverage of these companies in each forum. We also investigate the association of keywords with each of these companies based on the post contents in the forums. In Section V, we provide the recommendations to improve the applicability and usefulness of the forums in raising public awareness to new scams, and to support the early detection of fraudulent merchants and activities, so as to enable a more pro-active approach in the handling of fraud and scams. We summarise the important findings in Section VI.

II. Collection of Data from Scam Reporting Forums

For our forum analysis research, we collect the contents from the following 6 scam reporting forums, namely exposeascam [20], realscam [21],scambaits [22], scambook [23], scamfound [24], and scamvictimsunited [25]. These forums allow users to post reports and complaints of their encounter with scam related incidents. We analyse the dates of the posts in the collected contents to obtain the first date of the post (i.e., a forum's start date) and the last date of the post (till the end date of our retrieval of all the posts from each forum) per forum, and compute their ages. However, an older age does not imply that a forum is more active. We extract the total threads and posts we find in each forum, and present the information together with the forum's age in Table I. We notice that the age of the forums differs very widely. We also notice that the activeness (i.e., the average threads/posts per day/week/month, and the gaps between no posting activity) of the forums differs too. Therefore, when conducting analysis in the subsequent sections, we will carry out normalization for a fair analysis when necessary.

Forum	Total Threads	Total Posts	Age (years)
exposeascam	2910	3439	1.07
realscam	1980	27264	2.28
scambaits	1677	9848	6.67
scambook	116430	116430	1.35
scamfound	242846	244248	3.08
scamvictimsunited	3354	16418	9.45

TABLE I: Forum Statistics

III. Keyword Based Analysis

To analyse the forum contents, we first generate a list of keywords to identify the applicability of scam related keywords in the detection of posts that provide details on the relevant incidents. From our observation of scam reports and consumer complaints online, we notice that the 28 keywords in Table II are often used. Therefore, we generate the list of keywords based on Table II for the keyword based analysis of the collected forums' data.

fraud	cheat	transaction	unfair
charge	liar	unauthorize	bill
rip-off	illegal	invalid	scam
fee	unethical	drug	compensate
hidden	attack	ripoff	refund
steal	unjust	unauthorise	porn
compensation	defect	damage	rip

TABLE II: Keyword List

Based on the keyword list, we analyse the forums' data and identify the posts that contain any of the keyword/s. Each word (separated by at least a word delimiter such as a space, tab, comma, full stop) is extracted from the post contents and a strict matching (i.e., not substring) with the keywords is applied. The keyword matching against the contents of the posts also provides us with the posts that are closely related to scam activities, for further analysis.

Next, we analyse the frequency of keywords found in the above identified posts. We analyse the posts to evaluate the keyword frequency by returning the post count for each keyword. In addition, we consider the large deviation in the forum sizes (i.e., number of threads/posts) and activeness, and thus carry out a normalization of the keyword frequency against the total posts per forum, to present the percentage of the identified posts containing each keyword per forum, in Table III. Note that each post may contain more than one keyword. Therefore, the total percentage per forum may be over 100%. We also compute and show the average normalized frequency of each keyword across all the forums. We observe that the top 10 keywords, in decreasing order according to their respective average normalized keyword frequency percentage, are scam, fee, fraud, damage, charge, rip, bill, refund, transaction, and liar. We can also see that 94.99% to 100% of the detected posts contain the keyword "scam" across all the 6 forums.

Next, we investigate the applicability and frequency of the combinations of keywords in the detection of scam related activities. We identify posts with contents that match any combination of the 28 keywords, and compute the number of posts matching a strict keyword combination (i.e., if the post content contains 3 different keywords, the post count will be incremented by 1 for this 3-keyword combination only. This computation is different from the 1-keyword based analysis where a post having 2 different keyword matches will have each post count incremented by 1 for each specific keyword. The keyword combination based analysis also ignores the order of the keyword appearance in the post contents.). We then extract the top 10 keyword combinations (based on the post counts) for each forum. To give a better view of the coverage of the detected posts on scam related activities based on each top keyword combination, we compute the normalized coverage in terms of percentage. The normalization is carried out over the total number of detected posts with any keyword occurrence.

The normalized coverage provided by the top 10 keyword combinations is shown in Table IV, with the total normalized coverage percentage for each forum shown in the last row of each sub-table (in bold). We observe from Table IV that with our chosen list of keywords, the top 10 keyword combination can identify 65.60% to 93.55% of the posts related to fraudulent and scam activities.

IV. Company Based Analysis

In this section, we analyse each forum based on their ability to identify popular companies mentioned in scam reporting forums. We retrieve the popular company list from the scambook forum. The scambook forum provides a list of the most popular companies based on their site's post data.

We retrieve the list of 1986 company names but notice that the list contains several names that may potentially generate high false positives (and false negatives) in our analysis results. Therefore, before we proceed, we clean up the company list according to the following steps (with real examples given from the original company list from the scambook forum).

1) Remove names with only numeric characters (e.g. 2012)
2) Remove all 1-character names
3) Remove all 2-character names if they contain only alphabetic characters (e.g. UK, SG, OK)
4) Remove trailing words if they are location name following a company name (e.g. ", London", ", Oxford") so that posts reporting a company in another location can also be detected
5) Remove trailing words if they are in short form and depict the company's liability or taxation type (e.g. Int'l, Ltd, LLP, Co, Inc, LLC)
6) Remove top level domain name if the company name is distinct enough without it (that is, do not remove the top level domain name if the company name is for example, cars.com or lends.net)

Other than cleaning up the company list by removing the less effective detection terms, we also generate new company names based on sub-string extraction of long company names if the original company names are too specific and may potentially results in high false negatives. An example is "Gameest Int'l Network Sales" where we additionally create another company name in the list for "Gameest". The final list contains 2019 company names.

As with the keyword based analysis, we also carry out a strict form of matching for the company based analysis. In addition, since we are carrying out the company based analysis using the company names generated from the scambook forum, we exclude this forum from some experiments in this section to remove the unfair bias in the analysis and evaluation.

First, we carry out an investigation on the number of company names that are reported in the post contents in each forum, and present the results in Table V.

We observe that there is no major overlap between the other forums and the scambook's existing reported companies, with the exception of the scamfound forum. 47.60% of the companies in the scambook forum can be seen as reported in the scamfound forum. To better analyse and conclude on the quality of the forums, it is necessary to understand if the other forums do detect other additional companies not included in the scambook forum's list (i.e., not reported by scambook members and users). However, the other forums do not provide a company name list compilation. A fair evaluation and comparison of all the forums should be carried out if such lists are provided in future.

Next, we identify the posts in each forum that report the companies in our list and compute the number of posts for each company per forum. We then identify the top 20 detected company names in each forum based on the number of posts reporting them. We observe from the results that some detected company names are not exactly distinctive as a company name. Some obvious examples are "not sure", "personal", "unknown" and "individual". It is important to note that if forums are to provide company name lists to aid in the detection of fraudulent and scam related activities, they need to be better maintained and cleaned up. Provision of such lists will be very useful in raising the awareness on the fraudulent merchants to look out for.

Another interesting observation from the results is the detection of legitimate companies such as McDonalds, Walmart

	exposeascam	**realscam**	**scambaits**	**scambook**	**scamfound**	**scamvictimsunited**	**Average Normalized Percentage**
attack	2.09	3.34	0.70	0.21	0.03	0.59	1.16
bill	13.99	5.19	4.49	15.25	2.20	2.99	7.35
charge	17.53	3.65	1.95	42.09	6.04	4.64	12.65
cheat	2.33	0.61	0.28	0.78	0.69	0.63	5.32
compensate	0.26	0.22	0.28	0.14	0.01	0.11	0.17
compensation	0.44	1.12	0.48	0.33	0.06	0.31	0.46
damage	2.27	1.51	0.41	100.00	0.47	0.54	17.61
defect	0.90	0.09	0.03	0.93	0.47	0.06	0.41
drug	0.87	0.78	0.47	0.28	0.15	0.35	0.48
fee	18.67	22.35	10.18	16.26	97.64	11.52	29.44
fraud	23.18	12.33	10.33	11.96	5.76	13.82	12.90
hidden	1.63	0.58	0.12	0.30	0.15	0.20	0.50
illegal	1.63	4.14	0.55	1.83	0.53	0.85	1.59
invalid	0.23	0.14	0.40	0.28	0.05	0.08	0.20
liar	2.65	2.85	0.84	1.08	0.41	1.21	1.51
porn	0.23	2.65	0.15	0.19	0.03	0.03	0.55
refund	14.36	1.53	0.20	13.89	2.40	1.73	5.69
rip	18.26	18.41	4.54	10.85	3.18	3.67	9.82
rip-off	0.55	0.21	0.02	0.19	1.31	0.03	0.39
ripoff	3.05	0.45	0.00	0.75	0.34	0.18	0.80
scam	100.00	99.99	99.92	100.00	100.00	94.99	99.15
steal	5.55	1.40	0.92	1.67	0.39	1.13	1.84
transaction	2.30	0.98	5.15	6.91	0.27	2.85	3.08
unauthorise	0.26	0.01	0.01	0.91	0.31	0.01	0.25
unauthorize	1.22	0.13	0.16	10.18	2.22	0.13	2.34
unethical	1.42	0.46	2.73	0.18	0.36	0.06	0.87
unfair	0.81	0.45	0.11	0.23	0.30	0.14	0.34
unjust	0.06	0.12	0.03	0.04	0.03	0.07	0.06

TABLE III: Normalized Keyword Frequency - Post Count Per Keyword (in Percentage)

exposeascam	**realscam**	**scambaits**
scam: 30.13	scam: 45.94	scam: 69.24
fraud,scam: 10.32	rip,scam: 10.63	fraud,scam: 5.59
fee,scam: 5.21	fee,scam: 10.20	fee,scam: 4.81
rip,scam: 5.21	fraud,scam: 5.47	bill,scam: 3.01
refund,scam: 4.01	bill,fee,scam: 1.48	fraud,scam,unethical: 2.52
charge,scam: 3.95	fee,rip,scam: 1.40	rip,scam: 2.46
bill,fraud,scam: 3.75	porn,scam: 1.20	fee,scam,transaction: 1.88
bill,scam: 1.48	illegal,scam: 1.26	scam,transaction: 1.36
attack,bill,fraud,scam: 1.42	fee,fraud,scam: 1.18	charge,scam: 0.57
charge,fee,scam: 1.31	bill,scam: 0.95	scam,steal: 0.43
66.79	**79.71**	**91.85**
scambook	**scamfound**	**scamvictimsunited**
damage,scam: 28.23	fee,scam: 75.96	scam: 64.80
charge,damage,scam: 12.63	fraud,scam: 4.61	fraud,scam: 8.22
damage,fee,scam: 3.76	charge,fee,scam: 3.52	fee,scam: 5.81
damage,refund,scam: 3.37	fee,refund,scam: 1.91	rip,scam: 1.56
bill,charge,damage,scam: 3.21	scam: 1.91	charge,scam: 1.49
damage,fraud,scam: 3.12	bill,fee,scam: 1.54	bill,scam: 1.24
bill,damage, scam: 3.04	charge,fee,scam, unauthorize: 1.23	fee,fraud, scam: 1.13
charge,damage,scam, unauthorize: 3.03	fee,rip,rip-off ,scam: 1.20	scam, transaction: 1.09
damage,rip,scam: 2.95	fee,rip,scam: 1.05	fee: 0.90
charge,damage,fee,scam: 2.28	fee,scam,unauthorize: 0.63	fraud: 0.73
65.60	**93.55**	**86.96**

TABLE IV: Top 10 Keyword Combinations for Each Forum (with Normalized Post Coverage in Percentage)

Forum	Number of Companies	Percentage of Companies
exposeascam	121	5.99
realscam	92	4.56
scambaits	54	2.67
scamfound	961	47.60
scamvictimsunited	79	3.91

TABLE V: Number and Percentage of Companies Detected in Forum

and Apple, with a high number of reported cases (i.e., in terms of the number of posts). A highly probable reason is the use of these legitimate platforms and their resources by scammers and fraudulent merchants to carry out scam related activities (e.g., advertising). In the case where these companies offer legitimate and highly popular products, the reports may also be associated with counterfeit products being advertised or sold as legitimate ones by the fraudulent merchants.

Other than that, we also observe that some companies are actually reported to be directly linked to complaints of scams and fraudulent activities. Some examples are C2 and C15 (as shown in Table VI), which have been reported in the forums to be associated with feedbacks such as delivering skin-care products that caused serious negative reactions, charging customers' credit cards without authorization, and/or recursively, or that they are uncontactable for feedback/refund thereafter.

Next, we carry out an analysis to identify the keywords associated with a selected set of the detected companies. By "associated", we do not mean that the keywords are indicative of the description of the company's activities. We mean that the keywords as well as the company name are within the contents of a same post.

For the company name and associated keyword analysis, we eliminate detected companies which do not have distinctive company names, or are well-established legitimate, high set-up cost companies, financial institutions and multi-national companies. We notice that the remaining companies are mainly online merchants or shops associated with multi-level marketing, pharmaceutical products, dating/matchmaking, advertising, etc. We extract the top keyword combination associated with each selected company name from each forum, consolidate them across all the forums, and present the selected companies from the top 20 detected companies and the associated keywords (as found in the post contents) in Table VI. In this table, company names are modified to preserve their identities as the objective of this analysis is simply to identify useful keywords associated with companies being flagged or complaint against.

While searching for the top keyword combination for the selected companies in the forums, we notice that even though some companies are not in the top 20 results of some forums, they do exist within the forums' post contents. We compile a list to indicate the presence or absence of the selected companies within each forum, and present the results in Table VI. Since the company list is generated from the scambook forum, it is excluded from this analysis.

From Table VI, we can see that there is a significant overlap in the presence of the detected top companies among the forums. However, the total overlap for most companies is minimal in some forums. Therefore, to enable a better detection of the fraudulent and scam related merchants and activities, we should rely on the detection results from multiple sources and carry out correlations, to obtain a better detection accuracy with a low false positive rate. There is also a need to eliminate false positives due to the wide presence of well-known legitimate sources. This elimination can be through a whitelist configuration and should only be implemented when it is definite that these companies do not provide resources that may be exploited by fraudulent merchants and scammers. However, a scenario that may not be avoidable is when scammers exploit the well-established reputation of such legitimate companies and use these company names to carry out malicious activities such as scamming and phishing.

V. Discussion

Based on this research and the observations, an important recommendation is the need for the provision of well-maintained fraudulent merchants or company list by scam reporting forums. The availability of this resource will enhance the value of these forums and fulfill their main purpose in providing readers with valuable information on the fraudulent merchants and scams to avoid. In addition, such lists and information could also be used by companies providing e-payment services to monitor the on-going status and reputation of their registered merchants, so as to take immediate action in the event of any violation of their terms and policies.

As our work is to investigate the possibility to raise public awareness to scams and fraud, and to enable the early detection of such malicious activities in the wild, it is necessary to ensure the quality of the detected results to prevent false triggering for investigations. The first and most important step would be to ensure the reliability and trustworthiness of the information from the online sources and forums. Scam reporting forums can incorporate moderation of the posts submitted to their forums to ensure that they are accurate through the provision of concrete supporting evidence (e.g. legal incident report, transaction statement) from the incident reporting user. This step may incur an additional overhead but is essential in ensuring the quality of the data in the forum.

VI. Conclusion

In this paper, we have carried out a fraudulent and scam related activity reporting forum data analysis. We collected the posts from 6 popular and active scam reporting forums, and generated a list of relevant keywords based on our preliminary analysis and knowledge of online sources on scam incident reporting. We then carried out an investigation on the ability to detect posts relevant to fraud and scams based on different keyword-based analysis scenario. We showed through our analysis that the choice of a single keyword can have an average coverage of 99.15% of the posts. However, the single keyword based detection can result in high false positives

Company	Associated Keywords	exposeascam	realscam	scambaits	scamfound	scamvictimsunited
C1	fee,scam				⋆	
C2	fee,scam				⋆	
C3	fee,fraud,scam,transaction			⋆	⋆	⋆
C4	charge,scam,transaction,unauthorise	⋆	⋆		⋆	⋆
C5	bill,charge,fee,scam,unfair	⋆			⋆	
C6	bill,charge,fee,illegal,refund,scam,unfair	⋆	⋆		⋆	
C7	fee,scam				⋆	⋆
C8	fee,scam				⋆	
C9	fee,fraud,scam			⋆	⋆	⋆
C10	fee,scam,unethical	⋆	⋆		⋆	⋆
C11	fee,fraud,scam	⋆		⋆	⋆	⋆
C12	fee,fraud,scam				⋆	
C13	fee,fraud,scam,steal		⋆		⋆	
C14	fee,scam				⋆	
C15	bill,fee,refund,rip,scam				⋆	
C16	fee,fraud,scam	⋆			⋆	⋆
C17	charge,fee,scam,unauthorize				⋆	
C18	fee,porn,scam,unauthorize,steal	⋆			⋆	⋆
C19	charge,fee,fraud,scam,transaction	⋆	⋆	⋆	⋆	⋆
C20	fee,illegal,scam				⋆	
C21	scam		⋆			

TABLE VI: Detected Individual Company and Associated Keywords in Post Contents, and Evidence of Presence of Detected Companies in Forums

when the detection feature is applied to generic online source. Therefore, we investigated the different keyword combinations and showed that the identification and selection of the top 10 keyword combinations is sufficient to support 65.60% to 93.55% coverage of the posts in the forums. We also evaluated the coverage of companies in the forums and investigated the association of keywords with each company. Our results showed that the merchant coverage in the forums is sufficiently wide for the identified popular companies. Based on our findings, we proposed some important recommendations to improve and enhance the applicability of forums and online sources in raising public awareness to new scams and fraud, and the early detection and prevention of such incidents to new potential victims.

References

[1] J. Zhang, M. S. Ackerman, and L. Adamic, “Expertise networks in online communities: structure and algorithms,” in *WWW Conference*, 2007, pp. 221–230.

[2] N. Glance, M. Hurst, K. Nigam, M. Siegler, R. Stockton, and T. Tomokiyo, “Deriving marketing intelligence from online discussion,” in *ACM SIGKDD International Conference on Knowledge discovery in Data Mining*, 2005, pp. 419–428.

[3] B. Bickart and R. M. Schindler, “Internet forums as influential sources of consumer information,” vol. 15, no. 3, pp. 31–40, 2001.

[4] S. Hariharan, R. Srimathi, M. Sivasubramanian, and S. Pavithra, “Opinion mining and summarization of reviews in web forums,” in *ACM Bangalore Conference*, 2010.

[5] Y. Zhang, S. Zeng, L. Fan, Y. Dang, C. A. Larson, and H. Chen, “Dark web forums portal: searching and analyzing jihadist forums,” in *IEEE International Conference on Intelligence and Security Informatics*, 2009, pp. 71–76.

[6] Y. Zhou, J. Qin, G. Lai, and H. Chen, “Collection of u.s. extremist online forums: A web mining approach,” in *Annual Hawaii International Conference on System Sciences*, 2007, p. 70.

[7] A. Abbasi and H. Chen, “Affect intensity analysis of dark web forums,” in *IEEE International Conference on Intelligence and Security Informatics*, 2007, pp. 282–288.

[8] A. Abbasi, H. Chen, and A. Salem, “Sentiment analysis in multiple languages: Feature selection for opinion classification in web forums,” vol. 26, no. 3, 2008.

[9] C. Yang, X. Tang, and B. Thuraisingham, “An analysis of user influence ranking algorithms on dark web forums,” in *ACM SIGKDD Workshop on Intelligence and Security Informatics*, 2010.

[10] R. Cai, J.-M. Yang, W. Lai, Y. Wang, and L. Zhang, “iRobot: An intelligent crawler for web forums,” in *WWW Conference*, 2008, pp. 447–456.

[11] Y. Wang, J.-M. Yang, W. Lai, R. Cai, L. Zhang, and W.-Y. Ma, “Exploring traversal strategy for web forum crawling,” in *ACM SIGIR International Conference on Research and Development in Information Retrieval*, 2008, pp. 459–466.

[12] J.-M. Yang, R. Cai, C. Wang, H. Huang, L. Zhang, and W.-Y. Ma, “A threadwise strategy for incremental crawling of web forums,” in *WWW Conference*, 2009.

[13] A. Sachan, W.-Y. Lim, and V. L. L. Thing, “A generalized links and text properties based forum crawling,” in *IEEE/WIC/ACM International Conference on Web Intelligence*, 2012, pp. 113–120.

[14] H.-M. Ying and V. L. L. Thing, “An enhanced intelligent forum crawler,” *IEEE Symposium on Computational Intelligence for Security and Defence Applications*, pp. 1–8, 2012.

[15] S. Li, L. Tang, J. Hu, and Z. Chen, “Automatic data extraction from web discussion forums,” in *Proceedings of the 2009 Fourth International Conference on Frontier of Computer Science and Technology*, 2009, pp. 219–225.

[16] S. Pretzsch, K. Muthmann, and A. Schill, “Fodex–towards generic data extraction from web forums,” in *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*. IEEE, 2012, pp. 821–826.

[17] J.-M. Yang, R. Cai, Y. Wang, J. Zhu, L. Zhang, and W.-Y. Ma, “Incorporating site-level knowledge to extract structured data from web forums,” in *WWW Conference*, 2009, pp. 181–190.

[18] W.-Y. Lim, A. Sachan, and V. L. L. Thing, “A lightweight algorithm for automated forum information processing,” in *IEEE/WIC/ACM International Conference on Web Intelligence*, 2013, pp. 121–126.

[19] W.-Y. Lim, V. Raja, and V. L. L. Thing, “Generalized and lightweight algorithms for automated web forum content extraction,” in *IEEE International Conference on Computational Intelligence and Computing Research*, 2013.

[20] Exposeascam, http://www.exposeascam.com.

[21] Realscam, http://www.realscam.com.

[22] Scambaits, http://www.scambaits.net.

[23] Scambook, http://www.scambook.com.

[24] Scamfound, http://www.scamfound.com.

[25] Scamvictimsunited, http://www.scamvictimsunited.com.

A New Approach to Improve Accuracy in Information Security Risk Management

Víctor Leonel Orozco López, Raul Ceretta Nunes
Computer Science Graduate Program (PPGI)
Federal University of Santa Maria (UFSM)
Santa Maria, RS, Brazil
e-mail: vlopez@inf.ufsm.br, ceretta@inf.ufsm.br

***Abstract*—Risk management constitutes a basis for decision making in a business continuity plan, since it creates a view that allows to identify and control risks that can compromise the assets of a given organization. Despite the existence of several methodologies to estimate the severity of these threats, preview evidence has demonstrated that the presence of human data sources for risk analysis can produce biased results, thus compromising the business continuity as a result of wrong-guided investments. In this work, we present an approach that reduces human biases by weighting risk evaluations using a reliability level of the sources, based on risk treatment performance. The experiments showed that the usage of reliability scores can effectively increase the accuracy of risk estimation, becoming a tool to minimize and/or eliminate those data sources that provoke the deviation of risk assessment results.**

Keywords–Business continuity; security; risk assessment; accuracy; decision making

I. Introduction

Business continuity management is a tool aimed to guarantee the delivery of services in presence of risk expositions. To achieve its goals, it requires the creation of a business continuity plan that describes strategies to control risks by mitigating their causes, effects and also ensuring the existence of contingent measures to reduce the impacts of catastrophic events [1].

Within the context of information security, the standard ISO 27005:2011 proposes the implementation of a risk management process that can be applied as a part of a business continuity plan [2], the main objective of which is to establish, prioritize and control those activities regarding to risks, enabling a balance between risk mitigation costs and risk mitigation actions.

One of the most important phases into a risk management program is the risk assessment phase, because the information generated at this stage guides all actions regarding to risks. The risk assessment phase is usually framed in two categories: quantitative risk assessments and qualitative risk assessments [3]. The last category has a significant prevalence because of the practical considerations in analysis and manipulation of data. Nevertheless, quantitative assessment claims for deterministic data. Thus, it is very common to map expert opinions to numerical values in terms of probabilistic functions [4].

Although the usage of expert opinions can provide information not perceptible with other sources, the data by itself could present biases due the subjective nature of human judgment [5], which in the context of information security means that security risks are wrongly estimated, leading to wrong investment and treatment actions.

To counteract this situation, this paper presents an iterative and incremental approach to improve the accuracy in risk assessments. Under the hypothesis that it is possible to establish the reliability score of a human opinion, we assume that reliability could be used to emphasize more reliable opinions, and propose a new approach to improve the performance of the resultant risk priorities.

For the measurement of the reliability levels, our work uses a combination of personalized views of trust and performance metrics as reputation, reducing the consequences in each risk assessment by refining the trust with updates based on risk treatment performance.

The rest of this paper is organized as follows. Section II introduces fundamental concepts for the scope of the paper and related work. Section III presents the approach for the increment of risk assessment accuracy. Section IV presents the experiments and results. Finally, Section V presents the conclusions of this work.

II. Background

A. *Risk management with ISO 27005:2011*

The ISO 27005:2011 risk management process is composed by eight phases that aim to define, estimate and control those risks that threaten the assets of an organization [2].

In a regular implementation of the standard, the process is executed following this sequence: first, the scope of the risk management is defined by the context definition phase; second, the risks are identified, their priority is estimated and the actions to counteract them are defined in the risk assessment phase; third, a decision is made to define which risks will be mitigated and which others will be assumed, inside the treatment and acceptance phases; then all the decisions and actions are communicated to all stakeholders, implementing also a monitoring and review phase. This cycle is repeated if the default time period between risk assessments has expired or if the risk indicators are not presenting satisfactory results, where the decision to start another cycle is dependent on the policy of each organization.

B. *From risk divergences to risk biases*

Since the standard ISO works as a code of practice, a variety of methods has been developed for each of its phases, and in phases like risk assessment these differences can lead to divergent results between methods. Then, aiming to create a representative result between a set of methodologies, Amaral et al. [5] proposed a composition of common assessment methods. The creation of this composition achieved a promissory normalization between the results of the methods, and it also evidenced that the results of risk assessments can be biased by the source of data, which in the case of the methods on the composition -Information Security Risk Analysis Method (ISRAM) [6], Austrian Risk Management Approach (ARIMA) [7], Failure Mode and Effect Analysis (FMEA) [8] and Automated Risk and Utility Management (AURUM) [9]- are interviews with experts, who had different background and competences that consequently led to biased risk opinions.

Although the selection of fully deterministic sources seems as the shortest path to eliminate biases, there are situations where is not possible to establish a “hard data source”, mostly because of lack of historical data regarding to risks. So, given the existence of environments where these opinions cannot be discarded, one way to affirm that the opinions are reliable depends on the expert himself, since the opinion generated by reliable origins is deemed as reliable [10].

However, the possibility to use the reliability of an expert inside its community, i.e., its trust score in relation to others is non-trivial. In fact, trust as a computational concept requires complex models with techniques like direct measurements, simple reputation models and recently social networks analysis [11].

C. Related works

The model presented by Workman [12] suggests that most of the security decision making literature is focused in situational factors, but it does not considers the biases that could affect these factors, suggesting that biases are a non solved research problem that needs more studies.

In the same context Banerjee [13], tries to reduce the biases by modifying the perceived scale of risks, based on the hypothesis that risk perceptions have a logarithmic behavior instead of linear, adjusting the mediocrity line of perceived risks.

With a managerial approach, Primão et al. [14] focuses the reduction of biases by using a controlled selection of risk assessment participants based on skills, using a contextualized definition of the required competences to be a risk assessment participant.

Focused on smart grids, Lopez et al. [15] proposes an alert mechanism that supervises patterns of behavior of the systems that belong to the smart grid. This mechanism generate alerts to trigger human actions, and most importantly, it assigns responsibilities for those actions by reputation scores. It recognizes the existence of individuals with different competences, using to construct the reputation with variables like feedback, criticality of the alert, operator’s workload and the time of response for the incident.

Finally, Khambhammettu et al. [16] presents a framework for risk assessment in access control systems, which focus their contributions on making authorization decisions by comparing security risks for access requests based on a four dimensional approach: object-sensitivity, subject-trustworthiness and two additional scopes combining sensitivity and trustworthiness.

This work differs from them by the following reasons: i) It presents an approach that improves accuracy by reducing biases with reliability; ii) It does not require a selection of participants of risk management based on skills; iii) It does not reconfigure the perception scales; iv) Since the reputation is context dependent, this work uses specific variables from risk management context; v) It presents a reliability based approach that can use diverse sources of initial trust.

III. Risk management with improved accuracy

A. Hypothesis and big picture

Considering that is possible determine the reliability level of a person within an organization, this approach uses this reliability to improve the accuracy of risk management by emphasizing the opinions of those members with higher reliability. The approach is built upon the fact that trust and risk are closely related concepts, because trust is the disposition that a person has to rely on another person’s opinions in relations that involve risks; namely a parameter that explains the ability of a person to estimate the risks severity in front of possibilities of deceptions and bad results [17].

To determine and use the reliability levels previous works were adapted, modifying their characteristics and introducing a social network analysis element as shown in Figure 1, that has as basis the work of Amaral et al. [5] in which the problem appeared.

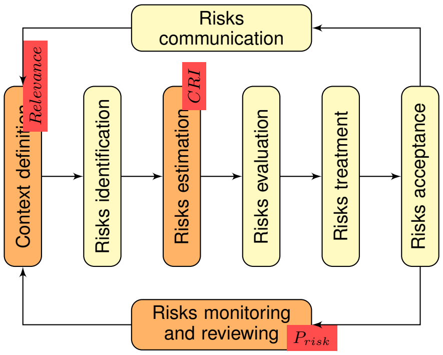


Figure 1. Trust based risk assessment.

This new version of the cycle uses the trust between members of the organization to determine the reliability of a person. For that, it is used an algorithm originally designed for recommender systems called TrustWebRank [18] adapting it to the risk assessment characteristics by remodeling its update function and presenting a global metric of reliability based on [19] ideas, denominated $Relevance$.

Once the $Relevance$ value is calculated, it is introduced into the risk assessment composition using a mathematical weight approach. This approach was selected because it overpasses the performance of other complex approaches while generating equivalent results [4]. From here, a coefficient that indicates the priority of a risk is obtained, denominated Composite Risk Index (CRI), that now reflects the evaluators reliability and is used to guide the investments.

To monitor and review the performance of the treatments, this approach uses Key Risk Indicators (KRI), present in many popular risk management methodologies like [20], representing instant metrics of risk events (those that facilitate apparition of risks).

Since the apparition of one risk can have multiple factors, the relation between KRI and $Risks$ is considered as many-to-many, thus this approach presents a performance indicator denominated Performance of risk (P_{risk}), based on the KRI benchmark presented by Talbot [21].

B. Interaction between components

For the creation of this approach, the following assumptions were taken: i) The computation of $Relevance$ is executed prior to any analysis activity, and the first execution is achieved using an initial trust in the form of witness information (WI), i.e., the actual trust among peers. Then, the subsequent $Relevance$ values are a product of an aggregation of direct observations (DO), i.e., the performance of subsequent risk management cycles and the original witness information (WI). Both kinds of trust are explained in [22]; ii) The organization structure is represented by an informal social network, conformed by links that represent the interaction between the organization's members who act as agents; iii) The organization is willing to monitor its risk treatment performance to update its trust perception based on results, there is not conspiratorial groups, and the risk management is performed by a risk management committee in behalf of all the peers and organization divisions.

The reliability level given to an agent inside a social network is formally defined as trust centrality, and TrustWebRank computes it based on the feedback centrality, meaning that the direct trust T_{ij} between an agent *i* to the opinions r of an agent *j* can be adjusted by using the trust between neighbors *k* of *i* for the agent *j* and the trust that *j* has for its neighbors *k*, giving as a result an indirect trust value $\tilde{T}_{ij}$.

Although TrustWebRank can be executed in a step-by-step style by every pair of nodes, their creators presented an alternative based on matrixes given by (1), where $\tilde{T}$ represents the matrix of indirect trust values calculated with TrustWebRank, I the identity matrix, β an adjustment factor, and S a stochastic matrix of direct trust normalized values given by (2). The value for β is explained with detail at Section IV.

$$\tilde{T} = (I - \beta S)^{-1} S \tag{1}$$

$$S_{ij} = \frac{T_{ij}}{\sum\limits_{k \in N_i} T_{ik}} \tag{2}$$

Then, to create a global reliability value to use it as weight in risk opinions, the personalized values are collapsed to a global metric $Relevance$ (R). The relevance R_i of an agent i inside the organization structure is defined as the average of the indirect trust values of every agent l that belongs to the group of agents N, where N is the group of agents that have a trust value for i above the threshold $\tau = 0.01$ (as established by [19]). The equation of $Relevance$ is presented in (3).

$Relevance$ value could also be used to select the risk assessment committee members (as it is used in the following sections). Nevertheless, a selection based solely on their trust score is not mandatory.

$$R_i = \frac{\sum\limits_{l \in N > \tau} \tilde{T}_{li}}{|N > \tau|} \tag{3}$$

After the context definition and reliability quantification, the identification phase takes place by using brainstorming techniques between the members of the risk committee. The risks are now evaluated by the members of risk committee giving their opinion about the probability(P), detection(D), frequency(F), impact(I) and severity(S) of each risk using a standardized interview with questions in form of likert scales of five steps (very low, low, medium, high, very high), aiming to map their opinions to numerical values.

Once that opinions were assessed, these are used to create a risk ranking based on priority. This step is achieved by using a variant of the original risk assessment composition, which now considers $Relevance$, as is presented in (4). .

$$\begin{aligned} ARIMA &= ((I + ((P-1) * 0.5)) * 100) * R_i/5 \\ ISRAM &= ((P * I) * 100) * R_i/25 \\ AURUM &= ((P * I) * 100) * R_i/100 \\ FMEA &= ((S * O * D) * 100) * R_i/125 \end{aligned} \tag{4}$$

In this version of the equations, the risk estimations are calculated for each risk using all methods of the composition, and the results are condensed by using (5), where MTR corresponds to methods' total result and Mr to the group of methods used in the composition. Note that a group of MTR values will be generated, with a size of $n_p * n_r$, where n_p corresponds to the quantity of participants in the risk assessment committee and n_r to the quantity of risks

To guide the decision-making process, MTR values are collapsed again to obtain a composite risk index (CRI) for every risk r, where r is given by the average of the group MTR_r that corresponds to the MTR results concerning to the risk r as (6) shows, obtaining as a result a list of CRI useful to sort risks by priority.

$$MTR = \frac{\sum\limits_{m \in M_r} m}{|M_r|} \tag{5}$$

$$CRI = \frac{\sum\limits_{i \in MTR_r} MTR_i}{|MTR_r|} \tag{6}$$

With the introduction of $Relevance$ as a weight, the interval of values for CRI tends to shrink, nevertheless, this condition is ignored because CRI value is used only as a comparator of itself, i.e., index and does not have any other numerical significance. Now, using the CRI values, the assessment committee defines the risks treatment strategy with four possible actions -reduce, avoid, retain and outsource-, existing also a need to define how the performance of these actions will be monitored. For that, a P_{risk} indicator in form of benchmark was created, comparing the ideal state or risk events to their actual state using KRI indicators as the comparable elements.

KRI indicators are instant measures of the status of events that could derive in risks, achieving its goal by capturing several representations of the state of those events between two risk assessment executions. Hence, the P_{risk} indicator for a risk r is modeled as the difference of the average of the group of values V_{MaxKRI} that contains the greatest value reached by every KRI that has relation with r and the average of the group of values V_{Ideal} that contains the ideal value for every KRI that has a relation with r, presented in (7).

$$P_{risk} = \frac{\sum\limits_{v \in V_{MaxKRI}} v}{|V_{MaxKRI}|} - \frac{\sum\limits_{v \in V_{Ideal}} v}{|V_{Ideal}|} \qquad (7)$$

In P_{risk} equation, if the average of V_{MaxKRI} exceeds or equals the average of the ideal state V_{Ideal} means that the risk was treated with good performance and P_{risk} value is positive. But, if the average of V_{Ideal} is above the average of V_{MaxKRI} means that the risk treatment was not enough to reach risk goals and probably the risk needed more investments.

With the measurement of risk treatment performance, it is possible to update the reliability of every participant based on the effectiveness of their opinion -i.e Direct Observations (DO)-. For that, TrustWebRank's equation of utility is simplified as $u_{ij} = P_{Risk}$, where j can be any agent that had an opinion about the risk, i.e., a member of the risk management committee, meaning that the trust of any agent i to the opinion of j is updated based on the results of the opinions of j.

For the purposes of risk analysis, it is desirable a *"slow positive-fast negative"* dynamic of trust, where the increment of trust is a slow process, but the decay in front of losses does not depend on many deception events [23]. This concept is achieved by introducing two trust limits $\kappa = 0.2$ and $\gamma = 0.6$ (established by simulation), a change from the original update intervals of TrustWebRank's function. Equation (8) formalizes the new update function, where $\breve{T}_{ij}$ corresponds to the updated direct trust value.

$$\breve{T}_{ij} = \begin{cases} T_{ij} + (1-\gamma)|P_{Risk}| \\ if\ P_{risk} > 0 \\ T_{ij} - (1-\kappa)|P_{Risk}| \\ if\ P_{risk} \leq 0 \end{cases} \qquad (8)$$

IV. Experiments

To state if our proposal effectively increases the accuracy of the risk assessment, we evaluated its performance comparing it to Amaral et.al. [5] approach. Both approaches were evaluated in a testbed to answer the following research questions:

- Does the accuracy of risk management is increased?
- Does the size of the committee represents influence?
- Does the approach reproduces the "slow positive-fast negative" behavior?
- Does the approach works against wrong trust scores?
- Is the initial trust a factor for the effectiveness?

For the execution of the testbed, it was necessary to select fair metrics of comparison and obtain them from a simulation.

A. Simulator

To create a simulation that avoids convergences to ideal but unrealistic results, the simulator combines a set of random but parameterizable generators for the trust between peers, treatment performance and risk opinions with a network generator algorithm. The architecture is detailed at Figure 2.

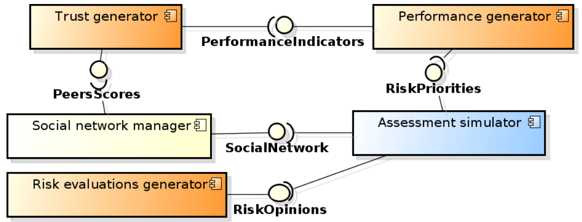


Figure 2. Simulator components

By using Kleinberg's small world algorithm [24] implemented with JUNG [25], the social network manager represents organizations' structures as social networks, selected due its usage of power-law distribution, commonly accepted as a good representation of real world social networks.

The generators of trust scores, performance metrics and the risk opinions were designed in a form that avoids any direct influence over the results using *profiles*, sets of intervals which represent sets of values that correspond to common conditions for every element of the simulation (behavioral profiles for trust scores, criticality of risks for risk evaluation and gain/loss profiles for risk treatments). The corresponding intervals of values for every profile are detailed at Table I.

TABLE I. Intervals of simulation profiles

Category	Profile ID	Interval
Trust profile	KNOWN	[0,0.3)
	COMPANION	[0.3,0.6)
	FRIEND	[0.6,1]
Risk evaluation profile	RANDOM	[very low, low, medium, high, very high]
	SECONDARY	[very low, low, medium]
	CRITICAL	[high, very high]
Performance profile	GOOD	[0,0.5)
	BAD	(-0.5,0)

B. Evaluation criteria

To achieve the creation of a fair testbed, we selected some indicators from CIS [26] as base of comparison, specifically those that have direct relation to risk management and can be adequately represented by simulation.

Incidents quantity. A high-priority risk that falls outside the first third of priorities is considered as incident due its likeness to receive few investments.

Cost of incidents. For illustrative purposes a fixed value of $ 1000 is attributed to every incident.

Time from discovery to containment. Represented as the number of steps to reach a zero value for $Relevance$, indicating the ability to discard bad opinions.

Also, to enhance the elimination of tendentious results, the simulator was configured to represent the following structure:

1) Social network size: 50 agents;
2) Risk assessment committee size: 10 agents;
3) Quantity of risks: 15 risks.
4) Priority of risks: 3 CRITICAL risks (r_1, r_2, r_3), others considered as SECONDARY risks;
5) Trust profiles: 2 agents with FRIEND profiles, others considered as COMPANION agents;

C. Preliminary simulations for trust dynamic

In order to define proper values for the control parameters described at section III-B, the simulator was configured to minimize the influence of relevance, treatment performance and risk estimations by producing fixed values. Latter, the simulator executed 10 continuous risk management cycles for 10 different values for each of the control parameters (γ, κ and β), using 0.1 as the distance between the evaluated values, obtaining the results presented in Figures 3, 4 and 5, which present the relevance of the risk committee participant with the higher initial trust value.

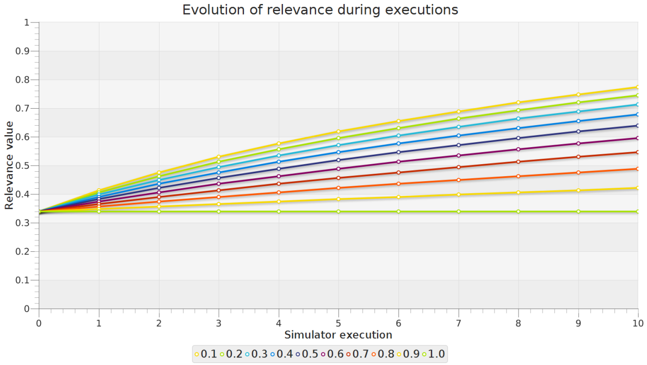


Figure 3. Relevance scores for different γ values

Figure 3 presents the evolution of relevance for γ. In this simulation, while larger is the value of γ, lower will be the speed with which the coefficient of relevance increases, reaching a point where there is no increase in the case that $\gamma = 0.1$. It can also be observed that the original value of TrustWebRank $\gamma = 0.6$ is located at an intermediate point between a rapid increase of trust and a lack of confidence trust, so it is conserved.

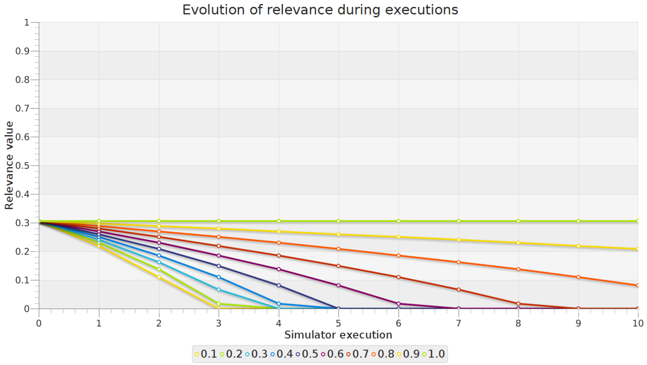


Figure 4. Relevance scores for different κ values

Figure 4 presents the evolution of relevance for different κ values. It is observed that while larger is the value of κ, lower is the decrement of relevance. Considering that a fast decrement of trust is desired to penalize wrong opinions, a value of $\kappa = 0.2$ was selected. With this value, it is possible to discard wrong opinions at the fourth execution, observing also a minimum relevance on third execution. This value was selected instead of $\kappa = 0.1$ to give a little margin for future modifications.

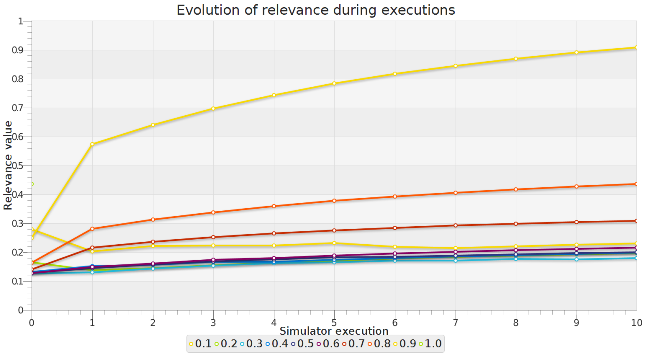


Figure 5. Relevance scores for different β values

Finally, Figure 5 presents the evolution of relevance for different β values. Unlike the previous simulations, the increase of β does not create an uniform variance of relevance. Is also noted that while most β values on the range [0,0.6] have similar behavior, those starting from $\beta = 0.7$ present a significant increment, being observed an intermediate value at $\beta = 0.8$ and an extreme value at $\beta = 0.9$. In consequence the $\beta = 0.8$ was selected.

D. Trust weight impact

Since the bias which affects the accuracy is caused by the proportion between good and bad opinions, this test aimed to state if the proportion between good risk evaluators and the committee size has an impact on the effectiveness. The simulator was configured to represent a bias like good opinions that are neglected by its proportion in relation to the total of opinions. Therefore, the simulations reproduced an assessment where the risk r_1, r_2 and r_3 are rated CRITICAL only by the agents with FRIEND profile, and as SECONDARY by the rest of the committee members; setting all other risks with a SECONDARY profile for all of the committee members.

With these parameters, we evaluated committees of different sizes from 6 to 18 members, testing 50 different graphs for every committee size; considering as a representative value of every size the sum of the incidents on all structures. Table II shows the results for two reliable opinions and Table III for four reliable opinions.

TABLE II. RISK COMMITTEE SIMULATIONS WITH TWO RELIABLE OPINIONS

Committee Size	Incidents Qty.	Est. Value	Incidents Qty. w/Trust	Est. Value w/Trust	Trust/ Original
6	22	$22,000.00	18	$18,000.00	0.82
7	25	$25,000.00	13	$13,000.00	0.52
8	26	$26,000.00	18	$18,000.00	0.69
9	34	$34,000.00	29	$29,000.00	0.85
10	38	$38,000.00	20	$20,000.00	0.53
11	37	$37,000.00	27	$27,000.00	0.73
12	37	$37,000.00	37	$37,000.00	1.00
13	47	$47,000.00	28	$28,000.00	0.60
14	48	$48,000.00	30	$30,000.00	0.63
15	52	$52,000.00	38	$38,000.00	0.73
16	45	$45,000.00	47	$47,000.00	1.04
17	56	$56,000.00	42	$42,000.00	0.75
18	48	$48,000.00	42	$42,000.00	0.88
	Total incidents	515	Total incidents	389	
	Value	$515,000.00	Value	$389,000.00	

From Table II, it can be observed that the relation *reliable agents/total agents* has a proportional influence on the

TABLE III. RISK COMMITTEE SIMULATIONS WITH FOUR RELIABLE OPINIONS

Committee Size	Incidents Qty.	Est. Value	Incidents Qty. w/Trust	Est. Value w/Trust	Trust/ Original
6	1	$1,000.00	0	$0.00	0.00
7	1	$1,000.00	0	$1,000.00	0.00
8	1	$1,000.00	0	$0.00	0.00
9	4	$4,000.00	1	$1,000.00	0.25
10	5	$5,000.00	0	$0.00	0.00
11	7	$7,000.00	2	$2,000.00	0.29
12	6	$6,000.00	1	$4,000.00	0.17
13	6	$6,000.00	4	$1,000.00	0.67
14	7	$7,000.00	2	$6,000.00	0.29
15	12	$12,000.00	7	$5,000.00	0.58
16	15	$15,000.00	5	$8,000.00	0.33
17	14	$14,000.00	8	$7,000.00	0.57
18	12	$12,000.00	6	$4,000.00	0.50
	Total incidents	91	Total incidents	36	
	Value	$91,000.00	Value	$39,000.00	

effectiveness of good opinions, where the number of incidents grows as the size of risk committee grows. This relation is also replicated by our approach, but it presented better results reaching a reduction of incidents with a relation of 389/515 = 0.76 (24% improvement of accuracy), representing a reduction of $11500 with the defined cost per incident.

In the same line, Table III shows that the increase of the quantity of reliable agents, also increased the accuracy of the assessments, generating a relation of 36/91 = 0.40 (60% improvement of accuracy) that represents an increase of 36% for the effectiveness in relation to the first test.

E. Resistance to bad bootstrap trust

A condition that was evident in the tests of past section is that under undesirable conditions like wrong trust scores between peers, the process can derive in wrong emphasis to opinions that could lead to poor results. Thus, to state the resistance of our approach in front of bad bootstrap opinions, we inverted the agents opinions, meaning that the two agents with FRIEND profile, qualify risks r_1, r_2, r_3 as SECONDARY (wrong qualification) and the other agents that present less $Relevance$, qualify them as CRITICAL (good qualification). Besides this, any other risks opinions were set as SECONDARY.

Figure 6 shows the variation of the $Relevance$ value for 10 consecutive executions over the same graph, presenting the evolution for the whole risk assessment committee. The simulation shown that $Relevance$ values for agent 29 and agent 11 suffered a decline as a consequence of their bad opinions, demonstrating that our process is able to adjust the relevance scores properly. Moreover, is observed that the relevance scores of the wrong opinions reached similar values to those presented by agents with good opinions in the second execution, and they were definitively eliminated at execution four, presenting also a “slow positive-fast negative” behavior.

F. Absence of bootstrap trust

Considering the existence of environments where peer trust measurement cannot be carried out easily, in this test we reconfigured the conditions from the previous section but now setting the trust between peers with a fixed value of 1.

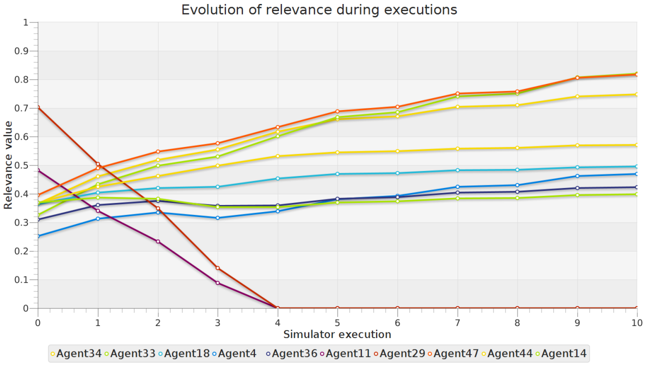


Figure 6. Relevance scores evolution over time

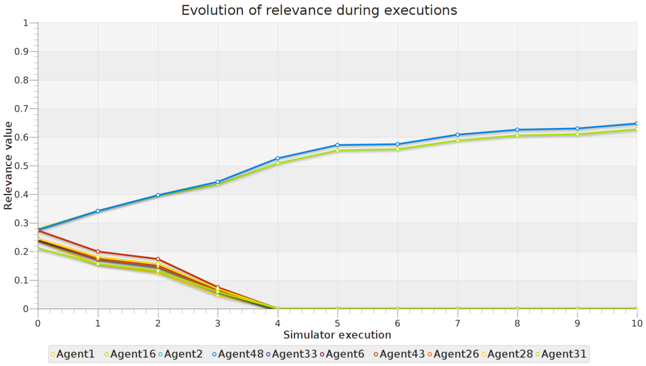


Figure 7. Relevance scores without bootstrap trust

Figure 7 shows that in presence of fixed trust opinions between peers, all agents receive almost uniform relevance values, presenting subtle differences as a product of the social network structure. Despite this, the simulations demonstrated that our procedure is still able to update the relevance scores, based solely on the subsequent events performance.

G. Non-linear evolution

The experiments presented above show that our approach achieves the desired behavior and effectiveness, thus we decided to run a test that considers change of opinions between executions of risk assessments. For this, we took as a basis the conditions presented in Section IV-E, but now, setting the risk evaluations as RANDOM. Generating the results presented at Figure 8.

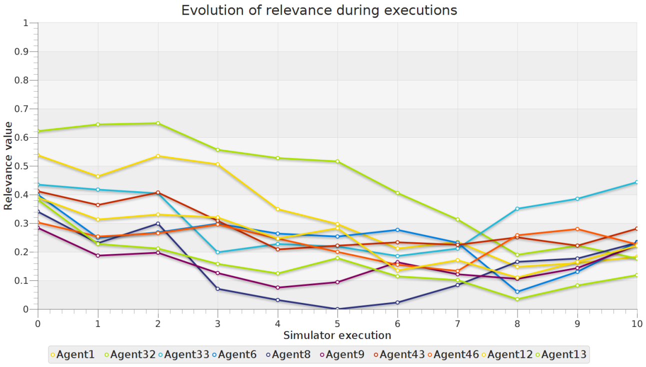


Figure 8. Relevance scores with random changes of opinion

ISBN: 978-1-61208-324-7

In Figure 8, it can be observed that negative performance results had a greater impact in relation to the positive performance results. However, the results also show that the trust update process managed properly the increases and decreases of trust, where those agents with constant bad opinions like agent 1 and 32 reached the mid section of relevance scores even though they were the peers with high relevance at beginning.

V. Final considerations

In this work, it was evidenced the importance of subjective data and its inconveniences for information security risk assessment methods. The usage of human subjective data can increase the risk computation biases and, consequently, compromise the business continuity.

To reduce the effects of this condition and increase the accuracy of risk management and consequently the business continuity, this work uses reliability as a mathematical weight to qualify human opinions about risks.

Simulation results showed that the emphasis on the reliable risk evaluators increases the accuracy of risk management, where the effectiveness of the approach lies in the relation *reliable agents/total agents*. The evidence showed that the solution has a proportional behavior with respect to the number of good reviews, achieving an accuracy increase of 25% for two reliable evaluators and 60% with four reliable evaluators.

The simulations also showed that the approach is resistant to wrong initial reliability, and the approach can be used without initial reliability scores at all, since the “slow positive - fast negative” update model is able to adjust the reliability.

Until now we have identified only two constraints of this approach. The first one is the absence of an ideal period of convergence for the trust updates, since every organization can have different policies for their risk assessment, i.e., monthly, quarterly, annually, dynamically. However, the simulations demonstrated that the approach can discard bad opinions in less than six executions, and there is a possibility to speed-up the update for good and bad treatments performance, with the κ and γ parameters that control the speed of the update. The second constraint is the fact that the solution executes its updates of trust based solely on performance results (because we aimed a fully independent approach).

In addition to work on the limitations, future works for the creation of more complex notions of trust are planned, to consider other dimensions of analysis like integrity, compliance, competencies, selfishness, reciprocity and others. Furthermore, it is suggested to evaluate the proposal with different trust quantification methodologies and risk assessment models, aiming to support other contexts with different characteristics that are not present on information security context.

References

[1] M. Blyth, Business Continuity Management: Building an Effective Incident Management Plan. Wiley, 2009.

[2] ISO, ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management, 2011.

[3] T. S. Coleman, A Practical Guide to Risk Management. Research Foundation of CFA Institute, 2011.

[4] R. T. Clemen and R. L. Winkler, “Combining Probability Distributions From Experts in Risk Analysis,” Risk Analysis, vol. 19, no. 2, 1999, pp. 187–203.

[5] E. H. Amaral, M. M. Amaral, and R. C. Nunes, “Risk Assessment Methodology by Composition of Methods,” in Brazilian Symposium on Information Security and Computer Systems, 2010, pp. 461–473.

[6] B. Karabacak and I. Sogukpinar, “ISRAM: information security risk analysis method,” Computers Security, vol. 24, no. 2, 2005, pp. 147–159.

[7] A. Leitner and I. Schaumuller-Bichl, “ARiMA - A New Approach to Implement ISO/IEC 27005,” in 2009 2nd International Symposium on Logistics and Industrial Informatics. IEEE, Sep. 2009, pp. 1–6.

[8] D. H. Stamatis, Failure mode and effect analysis: FMEA from theory to execution. ASQ Quality Press, 2003, vol. 38, no. 1.

[9] A. Ekelhart, S. Fenz, and T. Neubauer, “AURUM : A Framework for Information Security Risk Management,” SciencesNew York, vol. 0, no. September 2008, 2009, pp. 1–10.

[10] D. Ko, L. Kirsch, and W. King, “Antecedents of knowledge transfer from consultants to clients in enterprise system implementations,” MIS quarterly, vol. 29, no. 1, 2005, pp. 59–85.

[11] R. S. Burt, M. Kilduff, and S. Tasselli, “Social network analysis: foundations and frontiers on advantage.” Annual review of psychology, vol. 64, Jan. 2013, pp. 527–47.

[12] M. Workman, “Validation of a biases model in strategic security decision making,” Information Management & Computer Security, vol. 20, no. 2, 2012, pp. 52–70.

[13] A. Banerjee, “Equivalence of Risk: A Mathematical Approach,” in The 29th International System Safety Conference, 2011.

[14] A. P. Primão, R. C. Nunes, and V. L. O. López, “Definition Risk Assessment Committee Based on Competencies,” in XII SEPROSUL South American Week of Industrial and Production Engineering, 2012, pp. 1–10.

[15] J. Lopez, C. Alcaraz, and R. Roman, “Smart control of operational threats in control substations,” Computers & Security, vol. 38, Oct. 2013, pp. 14–27.

[16] H. Khambhammettu, S. Boulares, K. Adi, and L. Logrippo, “A Framework for Risk Assessment in Access Control Systems,” Computers & Security, no. Sec 2012, Apr. 2013, pp. 1–18.

[17] M. Lund, B. r. Solhaug, and K. Stø len, “Evolution in relation to risk and trust management,” Computer, 2010, pp. 49–55.

[18] F. E. Walter, S. Battiston, and F. Schweitzer, “Personalised and dynamic trust in social networks,” Proceedings of the third ACM conference on Recommender systems - RecSys ’09, 2009, p. 197.

[19] J. Chandra, I. Scholtes, N. Ganguly, and F. Schweitzer, “A Tunable Mechanism for Identifying Trusted Nodes in Large Scale Distributed Networks,” in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, Jun. 2012, pp. 722–729.

[20] ISACA, The Risk IT Framework. ISACA, 2009.

[21] M. J. Talbot, How to Performance Benchmark Your Risk Management: A practical guide to help you tell if your risk management is effective. CreateSpace Independent Publishing Platform, 2012.

[22] I. Pinyol and J. Sabater-Mir, “Computational trust and reputation models for open multi-agent systems: a review,” Artificial Intelligence Review, vol. 40, no. 1, Jul. 2011, pp. 1–25.

[23] C. Jonker and J. Treur, “Formal analysis of models for the dynamics of trust based on experiences,” in 9th European Workshop on Modelling Autonomous Agents in a Multi-Agent World, MAAMAW’99, 1999, pp. 221–231.

[24] J. Kleinberg, “The small-world phenomenon,” in Proceedings of the thirty-second annual ACM symposium on Theory of computing - STOC ’00. New York, New York, USA: ACM Press, 2000, pp. 163–170.

[25] J. O’Madadhain, D. Fisher, and P. Smyth, “Analysis and visualization of network data using JUNG,” Tech. Rep. Ii, 2005.

[26] The Center for Internet Security, “CIS Security Metrics,” The Center for Internet Security, Tech. Rep. 28, 2010.