IARIA

ICNS 2017

The Thirteenth International Conference on Networking and Services

ISBN: 978-1-61208-554-8

May 21 - 25, 2017

Barcelona, Spain

ICNS 2017 Editors

Kevin Daimi, University of Detroit Mercy, USA

Mary Luz Mouronte Lopez, Universidad Politecnica de Madrid, Spain

György Tamas Kalman, Norwegian University of Science and Technology, Norway

ICNS 2017

Foreword

The Thirteenth International Conference on Networking and Services (ICNS 2017), held between May 21 - 25, 2017 - Barcelona, Spain, continued a series of events targeting general networking and services aspects in multi-technologies environments. The conference covered fundamentals on networking and services, and highlighted new challenging industrial and research topics. Network control and management, multi-technology service deployment and assurance, next generation networks and ubiquitous services, emergency services and disaster recovery and emerging network communications and technologies were considered.

IPv6, the Next Generation of the Internet Protocol, has seen over the past three years tremendous activity related to its development, implementation and deployment. Its importance is unequivocally recognized by research organizations, businesses and governments worldwide. To maintain global competitiveness, governments are mandating, encouraging or actively supporting the adoption of IPv6 to prepare their respective economies for the future communication infrastructures. In the United States, government's plans to migrate to IPv6 has stimulated significant interest in the technology and accelerated the adoption process. Business organizations are also increasingly mindful of the IPv4 address space depletion and see within IPv6 a way to solve pressing technical problems. At the same time IPv6 technology continues to evolve beyond IPv4 capabilities. Communications equipment manufacturers and applications developers are actively integrating IPv6 in their products based on market demands.

IPv6 creates opportunities for new and more scalable IP based services while representing a fertile and growing area of research and technology innovation. The efforts of successful research projects, progressive service providers deploying IPv6 services and enterprises led to a significant body of knowledge and expertise. It is the goal of this workshop to facilitate the dissemination and exchange of technology and deployment related information, to provide a forum where academia and industry can share ideas and experiences in this field that could accelerate the adoption of IPv6. The workshop brings together IPv6 research and deployment experts that will share their work. The audience will hear the latest technological updates and will be provided with examples of successful IPv6 deployments; it will be offered an opportunity to learn what to expect from IPv6 and how to prepare for it.

Packet Dynamics refers broadly to measurements, theory and/or models that describe the time evolution and the associated attributes of packets, flows or streams of packets in a network. Factors impacting packet dynamics include cross traffic, architectures of intermediate nodes (e.g., routers, gateways, and firewalls), complex interaction of hardware resources and protocols at various levels, as well as implementations that often involve competing and conflicting requirements.

Parameters such as packet reordering, delay, jitter and loss that characterize the delivery of packet streams are at times highly correlated. Load-balancing at an intermediate node may, for example, result in out-of-order arrivals and excessive jitter, and network congestion may manifest as packet losses or large jitter. Out-of-order arrivals, losses, and jitter in turn may lead to unnecessary retransmissions in TCP or loss of voice quality in VoIP.

With the growth of the Internet in size, speed and traffic volume, understanding the impact of underlying network resources and protocols on packet delivery and application performance has assumed a critical importance. Measurements and models explaining the variation and interdependence of delivery characteristics are crucial not only for efficient operation of networks and network diagnosis, but also for developing solutions for future networks.

Local and global scheduling and heavy resource sharing are main features carried by Grid networks. Grids offer a uniform interface to a distributed collection of heterogeneous computational, storage and network resources. Most current operational Grids are dedicated to a limited set of computationally and/or data intensive scientific problems.

Optical burst switching enables these features while offering the necessary network flexibility demanded by future Grid applications. Currently ongoing research and achievements refers to high performance and computability in Grid networks. However, the communication and computation mechanisms for Grid applications require further development, deployment and validation.

We take here the opportunity to warmly thank all the members of the ICNS 2017 Technical Program Committee, as well as the numerous reviewers. The creation of such a 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 ICNS 2017.

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 ICNS 2017 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that ICNS 2017 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the fields of networking and services.

We are convinced that the participants found the event useful and communications very open. We also hope that Barcelona provided a pleasant environment during the conference and everyone saved some time for exploring this beautiful city.

ICNS 2017 Chairs:

Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Carlos Becker Westphall, Federal University of Santa Catarina, Brazil
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Mary Luz Mouronte Lopez, Universidad Politecnica de Madrid, Spain
Massimo Villari, Universita' di Messina, Italy
Éric Renault, Institut Mines-Télécom - Télécom SudParis, France
Robert Bestak, Czech Technical University in Prague, Czech Republic
Young-Joo Suh, POSTECH (Pohang University of Science and Technology), Korea
Gledson Elias, Federal University of Paraíba (UFPB), Brazil
Rui L.A. Aguiar, University of Aveiro, Portugal
Ivan Ganchev, University of Limerick, Ireland / Plovdiv University "Paisii Hilendarski", Bulgaria

ICNS Industry/Research Advisory Committee

Steffen Fries, Siemens, Germany
Alex Sim, Lawrence Berkeley National Laboratory, USA
Lorenzo Mossucca, Istituto Superiore Mario Boella, Italy
Jeff Sedayao, Intel Corporation, USA
Juraj Giertl, T-Systems, Slovakia

ICNS 2017

Committee

ICNS Steering Committee

Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Carlos Becker Westphall, Federal University of Santa Catarina, Brazil
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Mary Luz Mouronte Lopez, Universidad Politecnica de Madrid, Spain
Massimo Villari, Universita' di Messina, Italy
Éric Renault, Institut Mines-Télécom - Télécom SudParis, France
Robert Bestak, Czech Technical University in Prague, Czech Republic
Young-Joo Suh, POSTECH (Pohang University of Science and Technology), Korea
Gledson Elias, Federal University of Paraíba (UFPB), Brazil
Rui L.A. Aguiar, University of Aveiro, Portugal
Ivan Ganchev, University of Limerick, Ireland / Plovdiv University "Paisii Hilendarski", Bulgaria

ICNS Industry/Research Advisory Committee

Steffen Fries, Siemens, Germany
Alex Sim, Lawrence Berkeley National Laboratory, USA
Lorenzo Mossucca, Istituto Superiore Mario Boella, Italy
Jeff Sedayao, Intel Corporation, USA
Juraj Giertl, T-Systems, Slovakia

ICNS 2017 Technical Program Committee

Rui L.A. Aguiar, University of Aveiro, Portugal
Mehmet Aksit, University of Twente, Netherlands
Markus Aleksy, ABB AG, Germany
Patrick Appiah-Kubi, University of Maryland University College, USA
Mohammad M. Banat, Jordan University of Science and Technology, Jordan
Meriem Kassar Ben Jemaa, National Engineering School of Tunis (ENIT), Tunisia
Carlos Becker Westphall, Federal University of Santa Catarina, Brazil
Robert Bestak, Czech Technical University in Prague, Czech Republic
Ateet Bhalla, Independent Consultant, India
Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Fernando Boronat Seguí, Universidad Politécnica De Valencia-Campus De Gandia, Spain
Safdar Hussain Bouk, Kyungpook National University, Daegu, Republic of Korea
Maria-Dolores Cano, Universidad Politécnica de Cartagena, Spain
José Cecílio, University of Coimbra, Portugal
Salimur Choudhury, Algoma University, Canada
Kwangsue Chung, Kwangwoon University, Korea
Jorge A. Cobb, University of Texas at Dallas, USA
Hugo Coll Ferri, Universidad Politecnica de Valencia, Spain
Kevin Daimi, University of Detroit Mercy, USA
Philip Davies, Bournemouth University, UK

David Defour, University of Perpignan, France
Eric Diehl, Sony Pictures Entertainment, USA
Abdennour El Rhalibi, Liverpool John Moores University, UK
Gledson Elias, Federal University of Paraíba (UFPB), Brazil
Juan Flores, University of Michoacan, Mexico
Steffen Fries, Siemens, Germany
Sebastian Fudickar, University of Oldenburg, Germany
Ivan Ganchev, University of Limerick, Ireland / Plovdiv University "Paisii Hilendarski", Bulgaria
Rosario G. Garroppo, Universita' di Pisa, Italy
Serban Georgica Obreja, University Politehnica Bucharest, Romania
Juraj Giertl, T-Systems, Slovakia
Veronica Gil-Costa, National University of San Luis, Argentina
Victor Govindaswamy, Concordia University Chicago, USA
Genady Ya. Grabarnik, St. John's University, USA
Hermann Hellwagner, Klagenfurt University, Austria
Enrique Hernández Orallo, Universidad Politécnica de Valencia, Spain
Khondkar R. Islam, George Mason University, USA
Imad Jawhar, United Arab Emirates University, Al Ain, UAE
Aymen Jaziri, Orange Labs, France
Maxim Kalinin, Peter the Great St. Petersburg Polytechnic University, Russia
Georgios Kambourakis, University of the Aegean, Greece
Kyungtae Kang, Hanyang University, Republic of Korea
Sokratis K. Katsikas, Center for Cyber & Information Security | Norwegian University of Science & Technology (NTNU), Norway
Wolfgang Kiess, DOCOMO Euro-Labs, Germany
Pinar Kirci, Istanbul University, Turkey
Jerzy Konorski, Gdansk University of Technology, Poland
Elisavet Konstantinou, University of the Aegean, Samos, Greece
Diego Kreutz, Federal University of Pampa, Brazil / University of Luxembourg, Luxembourg
Francine Krief, Bordeaux INP, France
Mikel Larrea, University of the Basque Country UPV/EHU, Spain
Yiu-Wing Leung, Hong Kong Baptist University, Hong Kong
Tonglin Li, Oak Ridge National Laboratory, USA
Jaime Lloret Mauri, Polytechnic University of Valencia, Spain
Albert Lysko, CSIR Meraka Institute, South Africa
Zoubir Mammeri, Toulouse University, France
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Daniel Marfil Reguero, Universidad Politécnica De Valencia-Campus De Gandia, Spain
Ivan Mezei, University of Novi Sad, Serbia
Mario Montagud Climent, Universitat Politècnica de València (UPV), Spain
Philip Moore, Lanzhou University / Shandong Normal University, China
Lorenzo Mossucca, Infrastructure and Systems for Advanced Computing (IS4AC) -Istituto Superiore Mario Boella, Italy
Mary Luz Mouronte Lopez, Escuela Tecnica Superior de Ingenieria y Sstemas de Telecomunicacion - Universidad Politecnica de Madrid, Spain
Arslan Munir, University of Nevada, Reno, USA
Ridha Nasri, Orange Labs, France
Gianfranco Nencioni, Norwegian University of Science and Technology (NTNU), Norway

Alberto Núñez Covarrubias, Universidad Complutense de Madrid, Spain
Kazuya Odagiri, Sugiyama Jyogakuen University, Japan
Tuan Phung-Duc, University of Tsukuba, Japan
Zsolt Polgar, Technical University of Cluj Napoca, Romania
Md Arafatur Rahman, University Malaysia Pahang, Malaysia
Scott Rager, Raytheon BBN Technologies, USA
Da Qi Ren, Futurewei Technologies Inc., USA
Éric Renault, Institut Mines-Télécom - Télécom SudParis, France
Panagiotis Sarigiannidis, University of Western Macedonia, Greece
Jeff Sedayao, Intel Corporation, USA
Alireza Shams Shafigh, University of Oulu, Finland
Alex Sim, Lawrence Berkeley National Laboratory, USA
Vasco N. G. J. Soares, Instituto de Telecomunicações / Instituto Politécnico de Castelo Branco, Portugal
Young-Joo Suh, POSTECH (Pohang University of Science and Technology), Korea
Yoshiaki Taniguchi, Kindai University, Japan
Chandrashekhar Thejaswi PS, Samsung Electronics, India
Ishan Vaishnavi, Huawei Technologies, Munich, Germany
Hans van den Berg, TNO / University of Twente, Netherlands
Ioannis Vardiambasis, Technological Educational Institute (TEI) of Crete, Greece
Vladimir Vesely, Brno University of Technology, Czech Republic
Massimo Villari, Universita' di Messina, Italy
Ferdinand von Tüllenburg, Salzburg Research Advanced Networking Center, Austria
Jin-Yuan Wang, Peter Grünberg Research Center | Nanjing University of Posts and Telecommunications, China
Junwei Wang, University of Hong Kong, Hong Kong
Michelle Wetterwald, HeNetBot, France
Cong-Cong Xing, Nicholls State University, USA
Anjulata Yadav, Shri G.S. Institution of Technology and Science, Indore, India
Sherali Zeadally, University of Kentucky, USA
Tao Zheng, Orange Labs China, China
Jiazhen Zhou, University of Wisconsin – Whitewater, USA
Ye Zhu, Cleveland State University, USA

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

Securing Ford Mobility System- GoodTurn 1
Katherine Snyder and Kevin Daimi

Comparative Analysis of Algorithms for Bandwidth Allocation in EPON 8
Mary Luz Mouronte Lopez

A Novel Passive Tracking Scheme Exploiting Adaptive Line of Sight Links 15
Deockhyeon Ahn, Jungpyo Lee, Chao Sun, and Youngok Kim

Load Experiment of the vDACS Scheme to Use between Plural Organizations for Applications to the Small and Medium Size Scale Organization 19
Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii, and Makoto Takizawa

Securing Ford Mobility System - GoodTurn

Katherine Snyder and Kevin Daimi
Computer Science and Software Engineering
University of Detroit Mercy
Detroit, USA
email: {snyderke, daimikj}@udmercy.edu

***Abstract*—Ford Mobility System, *GoodTurn*, is an application developed by the University of Detroit Mercy through a Ford Motor Company grant. In a manner similar to Uber, the application connects Ford employees interested in volunteering their time and vehicles with nonprofit organizations needing to transport goods and resources. Both drivers and requesters will use their iPhones to connect to the application and each other. The privacy of the data collected from drivers, requesters, and the nonprofit organizations is critical. The goal of this paper is to introduce the needed security protocols to protect the GoodTurn application. The proposed security protocols will rely on the advocated GoodTurn security architecture.**

Keywords—Security Architecture; Security Protocol, Symmetric Cryptography; Public Key Cryptography; Ford Mobility System(GoodTurn)

I. Introduction

Ford Motor Company offered a program to solicit ideas from their employees regarding the best ways to serve the society at large and chose three of these projects to fund. The program was carried out in both USA and UK. One of the ideas presented was to have Ford employees donate their spare time and vehicles to help nonprofit organizations in moving their goods and resources. Given the existing support for iPhones by Ford for its employees, the initial release of the application was specified to use iOS, with the intention to expand to other devices and systems in later versions. The idea for the application was reminiscent of the way the Uber application connects drivers with riders, but with no money exchanged. Ford Motor Company provides a grant to develop this system and the University of Detroit Mercy was selected to develop and implement the application, currently referred to as the Ford Mobility System, *GoodTurn*. Xcode [1] was used to develop the GoodTurn application, based on the Swift language [2]. Furthermore, Firebase 3.0 was employed for several components of the application [3].

As stated above, the idea for this application was modelled after Uber. However, the security approach followed by this paper has nothing to do with Uber. The security of Uber has not been made public to allow others to compare their own security approaches to Uber. There has been some controversy about the operation and use of Uber. In 2015, McCallion [4] stressed that Uber has accidentally leaked the private information of many of its drivers when the app was newly launched. This initial release of the Uber app apparently had a design defect that allowed drivers to access various sensitive scanned documents containing details such as, social security numbers, tax forms, insurance documents, and drivers' licenses. The bug emerged when an Uber driver tried to upload or edit such documents. The driver was directed to a screen containing details of Uber drivers within the United States.

Bernstein [5] and Kovacs [6] indicated that a Portuguese team has recently found 14 flaws in Uber apps which have enabled the team to obtain free rides and access details of passengers and drivers. Another flaw detected by the team was linked to Uber's promotion codes. The riders.uber.com website did not involve any countermeasures against brute-force attacks. This flaw enabled attackers to continue to create promo codes until valid codes were obtained. With the emergent attractiveness of developing Uber-style applications, the attempts to use Uber as a development platform for various applications accessible via the cloud, requires more vigilant attention to security issues.

Armerding [7] emphasized that scammers attacking Uber can get a free ride, while victims pay the the bill. This occurred when cyber attackers manage to obtain the login credentials of legitimate users and sell them to fraudsters. Popular apps like Uber are targets for online scammers and cybercriminals; therefore, these apps must employ rigorous security and privacy measures to deter and prevent these malicious activities. Taking into consideration the above-mentioned incidents regarding Uber security, Uber continues to introduce app improvements with the aim of further securing the application and safeguarding privacy of drivers and passengers. Cava [8] stated that Uber added a new feature requiring drivers to authenticate their identities via a selfie photo prior to each shift. The goal of such real-time ID proof is to thwart fraudulent utilization of a driver's account and provide passengers with a higher degree of confidence in using Uber vehicles.

With the constantly increasing sophistication of security threats and attacks on software applications, advances in security countermeasures should at least parallel this sophistication. Dong, Peng, and Zhao [9] suggested using security patterns to avoid security problems. They believed that security patterns provide professional solutions to common security problems and capture best practices on secure software design and development. Security risk analysis is definitely the first step to design a secure system.

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-554-8

Baca and Petersen [10] introduced the notion of countermeasure graphs — a risk analysis approach for software security. They added that countermeasure graphs grant decision support for prioritizing countermeasures, and support software developers in determining critical threats and implementing optimal solutions. A Case-Based Management System (CBMS) comprised of an artifact management system and a knowledge-based management system (KBMS) to handle cases for secure software development was introduced by Saito, et al. [11]. The goal was to manage the software artifacts created in the secure software life cycle, in addition to the software security knowledge using the two components of CBMS. Although useful in secure software development, nevertheless, none of these approaches addressed secure communication between the software itself and its external interface.

Software security vulnerabilities give rise to many security breaches and attacks. New security vulnerabilities are discovered daily. Vulnerabilities are behind many software failures. In any software development, coding is the critical issue because many security deficiencies are developed during the coding phase. Okun, Guthrie, Gaucher, and Black [12] investigate the use of static analyzers to identify defects in source code that could result in security breaches. Jain and Ingle [13] argued that to have secure software, a software security requirements process is essential. They designated a Software Security Requirements Gathering Instrument (SSRGI) and claimed it can help developers extract security requirements from various stakeholders, and indicated SSRGI can strengthen security during the consequent phases of software development. Software security testing plays an important role in detecting security flaws. According to Tian-Yang, Yin-Sheng, and You-Yuan [14], Software security testing is the process of identifying whether the security attributes of software implementation are consistent with the design. They stipulated that software security testing involves security functional testing and security vulnerability testing. Security functional testing analyzes whether the software security attributes are implemented appropriately and consistently with security requirements. While testing for vulnerabilities and security flaws are essential for secure development, they do not necessarily prevent security attacks where software applications are accessed via the internet.

This paper presents a security architecture for the Ford Mobility System, *GoodTurn*. A cryptographic protocol is used to implement the security architecture. A protocol is a multi-party technique represented as a sequence of steps that exactly identifies the actions required of two or more parties in order to accomplish a specified goal. Mainly, the goal is to secure the exchange of messages between the parties. If cryptography is used to secure messages, a cryptographic protocol will be involved. Protocols are probably the most difficult part of cryptography because neither the designer nor the implementer of the protocol has any control over other parties' behavior. Normally, it is very challenging to isolate the vulnerabilities of cryptographic protocols as they can be the outcome of subtle design flaws [15]-[17]. The remainder of the paper is organized as follows: Section II provides the FMS operation overview. Section III elaborates on the FMS security architecture. Section IV depicts the cryptographic protocols needed to secure the FMS. Section V concludes the paper.

II. FMS OPERATION OVERVIEW

The following use case scenario briefly illustrates the operation of the Ford Mobility System, *GoodTurn*. This is needed to understand the security architecture of GoodTurn and the associated cryptographic protocol. Volunteer drivers will be referred to as "driver". A representative of the nonprofit requesting a driver to move goods will be referred to as "requester".

1. The system starts with a splash screen to indicate the application is being launched.
2. New drivers/ requesters register with the system first.
3. The application requests the user name and the password of the user (driver/requester). Subsequent use is authenticated against this information.
4. Driver/requester can modify their information/profile.
5. If needed, the system can recover password, deactivate or reactivate user account.
6. Non-profit organization/Non-government organization (NPO/NGO) adds and removes requester users, and provides them with administrative rights
7. Drivers and requesters sign off on a privacy policy.
8. The system provides a list of current jobs to drivers provided by requesters to move goods.
9. The system calculates the estimated time needed to complete a job by a driver.
10. Requesters enter new jobs, include their organization information, add a job to job queue, modify a job request, or cancel a job.
11. If a requester/driver does not want to deal with a specific driver/requester, the driver/requester is added to that driver/requester's blacklist. At any time, driver/requester can be removed from a black list.
12. Driver/requester view the job history.
13. Drivers filter jobs, sort them in any way they prefer, accept jobs, reject jobs or cancel accepted jobs. As a result, the job list is updated.
14. The system notifies the requesters/drivers regarding any action listed in step #13.
15. If a requester's job reaches its pick-up time without being accepted, the system will allow the requester to reschedule it.
16. The driver/requester indicates that a job is completed.
17. FMS allows communication between requester and driver.

18. Both drivers and requesters provide feedback, submit problems if any, and ask for help.
19. Drivers and requesters rate each other.

III. GOODTURN SECURITY ARCHITECTURE

The Ford Mobility System (GoodTurn) security architecture introduced in Figure 1 illustrates all the components used. The participating parties are shown in Table 1 below. Furthermore, Table 2 provides a clarification of the symbols used.

A. Key Distribution Center

The Key Distribution Center (KDC) is the heart of the security architecture. It manages the symmetric keys distribution for each pair of the communicating parties, and providing the needed public keys for communicating parties. It further provides the keys needed for Message Authentication Code (MAC), which will be used for ensuring the integrity of various exchanged messages. The designated Security Service Agent (SSA) will act on behalf of host and servers it represents. Any of the servers or hosts of Fig. 1 can request communication with the components they are allowed to communicate with. Because some of the messages are relatively large and others are small, symmetric and public key cryptography will be used respectively. The request for keys should include the ID of the party to communicate with and the type of key. There are two types of keys, session key and MAC key. The MAC key will be used for message authentication. The SSA of the requesting party asks the Key Distribution Center for a session key, K_{XY}, to be shared between components X and Y to be sent to the component requesting it. Here X is the requesting component and Y is the component that X needs to communicate with. The KDC send the session key to party X together with the ID of the other party and type of key so that each party knows whom it will be communicating with and what will the key be used for. In what follows, ID_X and ID_Y are the IDs of component X and Y respectively, Key Type is 1 for session key and 2 for MAC key, and SSA_X is the SSA for component X. Note X and Y stand for Application server, Database Server, NPO/NGO, Driver or Requester. K_S is the symmetric key shared by KDC and SSA_X. Note that → indicates sending, and || stands for concatenate.

$$SSA_X \rightarrow KDC: E\ [K_S, \text{Request for Key} \ || \ ID_X \ || \ ID_Y \ || \ \text{Key Type}]$$

$$KDC \rightarrow X: E\ [K_S, K_{XY} \ || \ ID_Y \ || \ \text{Key Type}]$$

It is assumed that KDC and SSA shared public keys. Upon successful login of a component, the component receives the public key of KDC, PU_{KDC} via its SSA. This is needed to contact the KDC when requesting various keys. The component X who has received the session key and MAC key will then request the public key, PU_Y, of the component Y it wishes to communicate with and waits for Y to confirm the connection. The public key of Y is needed by X to share the session key and MAC key with Y. The protocol to achieve that is as follows:

1. X sends its ID and the ID of Y encrypted with the public key of KDC. A nonce, N_X is needed for assurance. A nonce is used by the sender to assure the receiver (party following →) the message is from sender.

$$X \rightarrow KDC: E\ [PU_{KDC}, ID_X \ || \ ID_Y \ || \ N_X]$$

2. KDC sends X the public key of Y together with ID of Y and its nonce, N_{KDC}, all encrypted with KDC's private key (signed) and then with the public key of X.

$$KDC \rightarrow X: E\ [PU_X, E\ (PR_{KDC}, ID_Y \ || \ PU_Y \ || \ N_X \ || \ N_{KDC})]$$

3. X contacts Y providing its ID, Y's ID, and a nonce N_X to show that the message is current. All these are encrypted with the public key of Y

$$X \rightarrow Y: E\ [PU_Y, ID_X \ || \ ID_Y \ || \ N_X]$$

4. Y verifies with KDC to see if it can communicate with X.

$$Y \rightarrow KDC: E\ [PU_{KDC}, ID_X \ || \ ID_Y \ || \ N_X]$$

5. If KDC confirms the message, it encrypts the public key of X, ID of X, and a time stamp T_{KDC}. Note that the message is first signed with PR_{KDC}, and then made confidential with PU_Y.

$$KDC \rightarrow Y: E\ [PU_Y, E\ (PR_{KDC}, ID_X \ || \ ID_Y \ || \ PU_X \ || \ T_{KDC})]$$

6. Y carries out the required decryptions and obtains PU_X. It informs X it is ready to communicate by encrypting a message containing the ID of X, ID of Y, and a nonce, N_Y encrypted with the public key of X.

$$Y \rightarrow X: E\ [PU_X, ID_X \ || \ ID_Y \ || \ N_Y]$$

7. At this point X shares the session key and the MAC key, KM_{XY}, with Y. Here the message is also signed by PR_X first and then confidentiality is enforced through encryption by PU_Y.

$$X \rightarrow Y: E\ [PU_Y, E\ (PR_X, ID_X \ || \ ID_Y \ || \ N_X \ || \ K_{XY} \ || \ KM_{XY})]$$

The session and MAC keys are valid for a single communication only. Fresh session and MAC keys are requested for subsequent communications. Note that in what follows, the communication with the Key Distribution Center will not be mentioned because it has already been taken care of in this section. For example, the Application Server communicates with five components including the KDC. The link with the KDC will be subtracted from the total number of links resulting in four links only.

B. *Application Server*

The Application Server (AS) runs the FMS, and therefore, controls all the functions of the system. It communicates with Database Server, NPO/NGO, Driver, and Requester components. To achieve all these communications securely, four session keys and four MAC keys are needed. Certainly, the Application Server could have also played the role of KDC in addition to its original role. However, it is safer to have independent server taking care of key distribution.

C. *Database Server*

The Database Server (DS) stores information about drivers, requesters, and NPO/NGO. In addition to profiles of the requesters and drivers, it keeps the blacklist of drivers and requesters, job history, active jobs, deactivated/reactivated user accounts, rejected jobs, and accepted jobs. The DS aids the Application Server in carrying out its job. From Fig. 1, it is clear that DS exchanges messages with the Application Server only. No other component is allowed to access the Database Server. Hence, one session key and one MAC key are needed.

D. *Non-Profit/Non-Government Organization*

Non-Profit Organization (NPO) / Non-Government Organization (NGO) component communicates with the Requester and with the Application Server. It adds and removes users and requests some reports and displays from the Application Server (AS). Two session keys and two MAC keys are needed for such interaction.

E. *Requester*

The Requester (R) should be associated with an NPO/NGO. It interacts with both the Driver and the Application server. The requester exchanges a number of messages with the Driver and Application Server. Some of these messages include registration, profile change, list of current job, privacy policy, job addition, job cancelling, feedback, blacklist addition, driver rating, and completed jobs. Because there are two connections, two session keys and MAC keys are needed.

F. *Driver*

The Driver (D) communicates with both the Application Server and the Requester to exchange various messages, such as registration, profile change, list of current jobs, privacy policy, accepted jobs, blacklist insertion, requester rating, and completed jobs. The driver needs two sessions keys and two MAC keys.

TABLE I. PARTICIPATING PARTIES

Symbol	Meaning
KDC	Key Distribution Center
SSA	Security Service Agent
NPO	Non-Profit Organization
NGO	Non-Government Organization
AS	Application server
DS	Database Server
R	Requester
D	Driver

IV. SECURING THE SYSTEM

The security of the FMS system relies on both symmetric and asymmetric cryptography. In addition, MAC keys are shared between the communicating parties. As noted above, the KDC will provide symmetric and MAC keys to the party initialing the communication. Then that party will request the public key of the receiver to forward the session and MAC keys. Several messages shared by the Driver and Requester components with the Application Server are similar. Those messages will not be repeated.

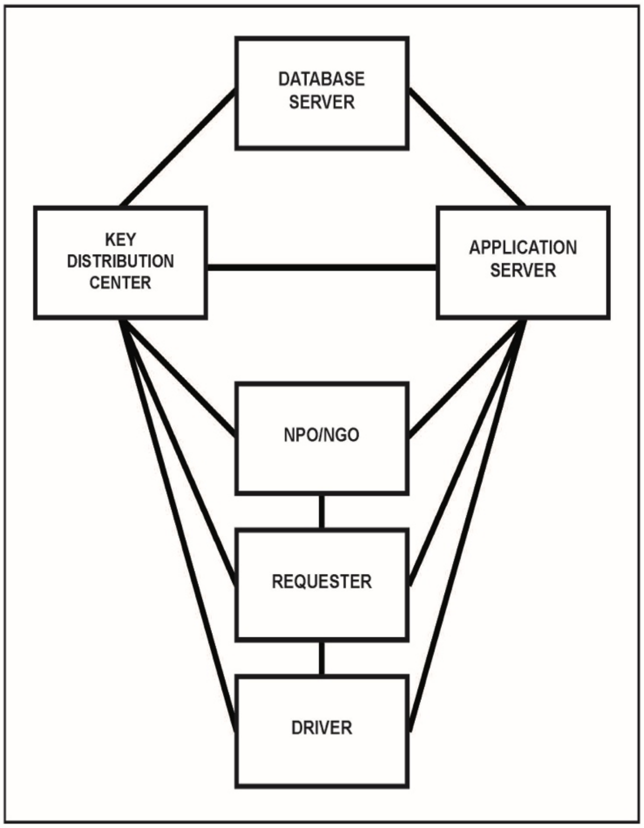


Figure 1. GoodTurn Security Architecture

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-554-8

A. *Driver-Server Communication*

The Driver component needs to send the following short messages to the Application Server (AS): email, password, security question/answer, request to reactivate account, request to register, registration information (name, email, driver/requester, address, company name, phone #, organization code, accepting/rejecting privacy policy, request to rate, rating, and job completed. All these messages are the same for the Requester (R). The symbol M will refer to any of these messages because the security procedure handling them is the same. D signs a message including its ID, ID of AS, M, the MAC of M (E ($KM_{D\text{-}AS}$, M)), and time stamp T_D, and then encrypt them all with the public key of AS, PU_{AS}

$$D \rightarrow AS\text{: } E\ [PU_{AS}, E\ (PR_D, ID_D \parallel ID_{AS} \parallel E\ (KM_{D\text{-}AS}, M) \parallel M \parallel T_D)]$$

On receiving such messages, AS performs the needed decryptions to obtain M. It then calculates the MAC of M and compares with the received MAC, and checks the currency of the message using T_D. Once they are equal, it accepts these messages and informs the Database Server (DS) to store the information or acts on them.

The Driver component also sends other messages that are specific to the Driver. They include vehicle make, model, year, color, license plate, type, maximum mileage, and messages to indicate job is accepted, job is rejected, and job is cancelled. These messages are treated as above.

The SA sends D messages that are somehow long, such as privacy policy, available jobs, accepted jobs list, cancelled jobs list, and completed jobs list. For this purpose, symmetric key will be adopted because public key tends to be slow with long messages. To this end, AS encrypts the ID of D, its ID, the MAC of message M, message M, and the time stamp T_{AS} with the symmetric key, $K_{D\text{-}AS}$, shared with D. T_{AS} is inserted to assure D the message is current

$$AS \rightarrow D\text{: } E\ [K_{D\text{-}AS}, ID_D \parallel ID_{AS} \parallel E\ (KM_{D\text{-}AS}, M) \parallel M \parallel T_{AS}]$$

D will decrypt this message using the key, $K_{D\text{-}AS}$, and verify the MAC and the message is current.

B. *Requester-Server Communication*

Most of the messages sent by the Requester, R, are the same as those sent by D. These are mentioned in the first paragraph of the Driver-Server Communication above. Here, a message is first signed with the private key of R, PR_R, and $KM_{R\text{-}AS}$ is the MAC key shared between R and AS.

$$R \rightarrow AS\text{: } E\ [PU_{AS}, E\ (PR_R, ID_R \parallel ID_{AS} \parallel E\ (KM_{R\text{-}AS}, M) \parallel M \parallel T_R)]$$

The requester transmits more messages that are specific to it. Some of these messages are: new job request, items to be moved, quantity, size of vehicle (truck, Sedan, SUV), load weight estimate (heavy, medium, light), pickup location, drop off location, date and time, ASAP, modify job, and reschedule job if not selected by driver. These are treated as above using the R → AS message. However, the requester has a long message to report a problem. This is treated using symmetric key, $K_{R\text{-}AS}$, which shared between R and AS, as follows:

$$R \rightarrow AS\text{: } E\ [K_{R\text{-}AS}, ID_R \parallel ID_{AS} \parallel E\ (KM_{R\text{-}AS}, M) \parallel M \parallel T_R]$$

The AS server disseminates the following messages to R: new password, credentials accepted, and privacy policy. New password and credentials accepted are communicated using public key. However, because the policy is long, symmetric key is used.

M_1 = New password | Credentials accepted

M_2 = Privacy policy

$$AS \rightarrow R\text{: } E\ [PU_R, E\ (PR_{AS}, ID_R \parallel ID_{AS} \parallel E\ (KM_{R\text{-}AS}, M_1) \parallel M_1 \parallel T_{AS})]$$

$$AS \rightarrow R\text{: } E\ [K_{R\text{-}AS}, ID_R \parallel ID_{AS} \parallel E\ (KM_{R\text{-}AS}, M_2) \parallel M_2 \parallel T_{AS}]$$

C. *Server-Database Communication*

In this communication, there are many frequent messages. In addition, both the AS and DS perform a lot of processing. Using public key will further slow the system. Therefore, symmetric key cryptology will be used.

The Application Server transmits the following messages to DS: request to verify password, user name, security Q/A, and registration information, deactivated/reactivated accounts, rating of both drivers and requesters, feedback, blacklist update, job history update, completed jobs list, and problems (lost item, complaint, vehicle feedback, broken link). Using M to refer to any of these messages, the message sent to DS can be represented as:

$$AS \rightarrow DS\text{: } E\ [K_{DS\text{-}AS}, ID_{DS} \parallel ID_{AS} \parallel E\ (KM_{DS\text{-}AS}, M) \parallel M \parallel T_{AS}]$$

On the other hand, DS transfers the following messages to AS: password verified, name verified, security Q/A, activation/deactivation info completed, rating stored, feedback stored, blacklist updated, driver job selection updates, requester requests for service, alerts on driver/requester of blacklisted requesters/drivers, removing from blacklist completed, privacy policy, list of completed jobs, and job history. The transferred message, M, is protected as follows:

$$DS \rightarrow AS\text{: } E\ [K_{DS\text{-}AS}, ID_{DS} \parallel ID_{AS} \parallel E\ (KM_{DS\text{-}AS}, M) \parallel M \parallel T_{DS})]$$

D. AS-NPO/NGO Communication

The NPO/NGO exchanges few messages with the Application Server. Three of which, request to add user, request to remove a user, and request to join, are short. Hence, public key is used. The third message, information about the organization, is large, and therefore, symmetric key is used.

M_1 = Request to add user | Request to remove user | Request to join
M_2 = Information about NPO/NGO

$$\text{NPO/NGO} \rightarrow \text{AS}: E\ [PU_{AS}, E\ (PR_{NPO/NGO}, ID_{NPO/NGO} \| ID_{AS} \| E\ (KM_{NPO/NGO\text{-}AS}, M_1) \| M_1 \| T_{NPO/NGO})]$$

$$\text{NPO/NGO} \rightarrow \text{AS}: E\ [K_{NPO/NGO\text{-}AS}, ID_{NPO/NGO} \| ID_{AS} \| E\ (KM_{NPO/NGO\text{-}AS}, M_2) \| M_2 \| T_{NPO/NGO}]$$

The AS server will forward these messages to the Database Server after carrying out the needed decryptions and verifying the MAC. The server will send acknowledgement messages to the NPO/NGO using public key cryptography.

E. Requester-NPO/NGO Communication

Normally, the Requester should join an NPO/NGO to be able to request moving goods and resources. Obviously, a message to get information about the organization before joining, and if the user is convinced, a message to request to add the user is issued. Obviously, “information about NPO/NGO” is large.

$$R \rightarrow \text{NPO/NGO}: E\ [PU_{NPO/NGO}, E\ (PR_R, ID_{NPO/NGO} \| ID_R \| E\ (KM_{NPO/NGO\text{-}R}, \text{add-user-info}) \| \text{add-user-info} \| T_R)]$$

$$R \rightarrow \text{NPO/NGO}: E\ [K_{NPO/NGO\text{-}R}, ID_{NPO/NGO} \| ID_R \| E\ (KM_{NPO/NGO\text{-}R}, \text{NPO-info}) \| \text{NPO-info} \| T_R]$$

F. Requester-Driver Communication

Communication between Driver and Requester is needed for last minute changes to the job, check list for delivered items, and delivered item status list (good condition, damaged). The secured messages forwarded by D to R are given below. Note that Check-out list can be small or large. To be safe, symmetric key is used.

M_1 = Check out list of delivered items

M_2 = Last minute changes (driver-side) | Approved last minute changes

$$D \rightarrow R: E\ [K_{D\text{-}R}, ID_D \| ID_R \| E\ (KM_{D\text{-}R}, M_1) \| M_1 \| T_D]$$

$$D \rightarrow R: E\ [PU_R, E\ (PR_D, ID_D \| ID_R \| E\ (KM_{D\text{-}R}, M_2) \| M_2 \| T_D)]$$

For the Requester to Driver communication, we have the following relations:

M_1 = Delivered item status list | signed check out list
M_2= Last minute changes (Requester-side) | Approved last minute changes

$$R \rightarrow D: E\ [PU_D, E\ (PR_R, ID_D \| ID_R \| E\ (KM_{D\text{-}R}, M_2) \| M_2 \| T_R)]$$

$$R \rightarrow D: E\ [K_{D\text{-}R}, ID_D \| ID_R \| E\ (KM_{D\text{-}R}, M_1) \| M_1 \| T_R]$$

TABLE II. SYMBOLS USED

Symbol	Meaning
PU_{AS}, PR_{AS}	Public and Private key of AS
PU_{DS}, PR_{DS}	Public and Private key of DS
$PU_{NPO/NGO}$	Public key of NPO/NGO
$PU_{NPO/NGO}$	Private key of NPO/NGO
PU_D, PR_D	Public and Private key of D
PU_R, PR_R	Public and Private key of R
$K_{D\text{-}R}$	Symmetric key shared by D, R
$K_{D\text{-}AS}$	Symmetric key shared by D, AS
$K_{R\text{-}AS}$	Symmetric key shared by R, AS
$K_{DS\text{-}AS}$	Symmetric key shared by DS, AS
$K_{NPO/NGO\text{-}AS}$	Symmetric key shared by NPO/NGO, AS
$K_{NPO/NGO\text{-}R}$	Symmetric key shared by NPO/NGO, R
MAC	Message Authentication Code
$KM_{D\text{-}R}$	MAC key shared by D, R
$KM_{D\text{-}AS}$	MAC key shared by D, AS
$KM_{R\text{-}AS}$	MAC key shared by R, AS
$KM_{DS\text{-}AS}$	MAC key shared by DS, AS
$KM_{NPO/NGO\text{-}AS}$	MAC key shared by NPO/NGO, AS
$KM_{NPO/NGO\text{-}R}$	MAC key shared by NPO/NGO, R
HDS	Historical data store
→	Then in Section III, Sends in section IV
← →	Both parties apply security requirements
T_D	Time stamp issued by D
T_R	Time stamp issued by R
T_{AS}	Time stamp issued by AS
T_{DS}	Time stamp issued by DS
$T_{NPO/NGO}$	Time stamp issued by NPO/NGO

V. CONCLUSION AND FUTURE WORK

This paper presented a security architecture for the Ford Mobility System, GoodTurn. To secure the communication between various components of this architecture, a cryptography protocol was adopted. Both symmetric key and public key cryptography were employed. Furthermore, Message Authentication Codes were relied upon. The suggested approach satisfied the security requirements; integrity, confidentiality, and authentication. The architecture will be tested and implemented when the Ford Mobility System, *GoodTurn*, is completed.

REFERENCES

[1] MacUpdate, “Xcode: Integrated Development Environment (IDE) for OS X,” https://www.macupdate.com/app/mac/13621/xcode, 2016, [retrieved: March, 2017].

[2] Swift Documentation, “The Swift Programming Language,” https://swift.org/documentation, 2006, [retrieved: March, 2017].

[3] Firebase, “Apple Success Made Simple,” https://firebase.google.com, [retrieved: March, 2017].

[4] J. McCallion, “Uber suffers massive security breach,” http://www.itpro.co.uk/data-leakage/25435/uber-suffers-massive-security-breach, 2015, ITPRO, 2015, [retrieved: March, 2017].

[5] P. Bernstein, “Bounty Hunters find Security Flaws in Uber Apps,” 2016, http://www.cloudsecurityresource.com/topics/cloud-security/articles/422447-bounty-hunters-find-security-flaws-uber-apps.htm, [retrieved: March, 2017].

[6] E. Kovacs, “Flaws Allowed Hackers to Access Uber Driver, Passenger Details,” http://www.securityweek.com/flaws-allowed-hackers-access-uber-driver-passenger-details, Security Week, 2016, [retrieved: March, 2017].

[7] T. Armerding, “Uber fraud: Scammer takes the ride, victim gets the bill,” http://www.csoonline.com/article/3059461/data-breach/uber-fraud-scammer-takes-the-ride-victim-gets-the-bill.html, CSO Online, 2016, [retrieved: November, 2017].

[8] M. Cava, “Uber to use driver selfies to enhance security,” http://www.usatoday.com/story/tech/news/2016/09/23/uber-use-driver-selfies-enhance-security/90859082/, USA Today, 2016, [retrieved: March, 2017].

[9] J. Dong, T. Peng, and Y. Zhao, “Automated Verification of Security Pattern Compositions,” Information and Software Technology, vol. 52, 2010, pp. 274-295.

[10] D. Baca and K. Petersen, “Countermeasure Graphs for Software Security Risk Assessment: An Action Research,” The Journal of Systems and Software, vol. 86, 2013, pp. 2411-2428.

[11] M. Saito, A. Hazeyama, N. Yoshioka, T. Kobashi, H. Wahizaki, H. Kaiya, and T. Ohkubo, “A Case-based Management System for Secure Software Development Using Software Security Knowledge,” Procedia Computer Science, vol. 60, 2015, pp. 1092-1100.

[12] V. Okun W. F. Guthrie, R. Gaucher, and P. E. Black, “Effect of Static Analysis Tools on Software Security: Preliminary Investigation,” in Proc. the 2007 ACM Workshop on Quality of Protection (QoP’07), Alexandria, Virginia, USA, 2007, pp. 1-5.

[13] S. Jain and M. Ingle, “Software Security Requirements Gathering Instrument,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 2, no. 7, 2011, pp. 116-121.

[14] G. Tian-Yang, S. Yin-Sheng, and F. You-Yuan, “Research on Software Security Testing,” International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 4, No. 9, 2010, pp. 1466-1450.

[15] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptology, CERC Press, 1997.

[16] N. Ferguson and B. Schneier, Practical Cryptology, John Wiley, 2003.

[17] T. Coffey and R. Dojen, “Analysis of a Mobile Communication Security Protocol,” in Proc. the first International Symposium on Information and Communication Technologies, Dublin, Ireland, 2003, pp. 322 – 328.

Comparative Analysis of Algorithms for Bandwidth Allocation in EPON

Mary Luz Mouronte López
Department of Software Engineering.
Universidad Francisco de Vitoria
Madrid, Spain
e-mail: maryluz.mouronte@ufv.es

Abstract—**In this paper we compare the main algorithms used for bandwidth allocation in Ethernet Passive Optical Networks (EPON): Interleaved Polling with Adaptive Cycle (IPACT), Constant Cycle Time (CCT) and Static Bandwidth Allocation for High Priority Services (SBAHPS) algorithms. Computer simulations are executed to reproduce the behavior of these methods using powerful software tools. Some changes in the computational procedures have also been implemented. The ICCT (Improved CCT) and SBAHPS algorithms showed the best results.**

Keywords-EPON; bandwidth allocation;resource efficiency.

I. INTRODUCTION

Traffic in telecommunication networks grows steadily because of data-intensive applications and services. To tackle this fact, EPONs have gained popularity as a suitable infrastructure to support such huge traffic in the access segment. In EPONs several Optical Network Units (ONUs) share a common upstream channel for transmission. The bandwidth must be dynamically allocated among multiple ONUs to achieve an efficient use of resources. Allocation algorithms take into account the instantaneous bandwidth demand and Quality of Service (QoS) requirements.

Dynamic Bandwidth Allocation (DBA) is an active field of research [1], and many different approaches have been proposed [2]-[12]. In this paper, we compare the main algorithms for bandwidth allocation for data transmission upstream from multiple ONUs to the Optical Line Termination (OLT) in EPONs [1], such as: IPACT, CCT and SBAHPS. Several indicators on efficiency and fair utilization of the EPON upstream bandwidth, while supporting the Quality of Service (QoS) requirements of different traffic classes, are calculated. Several modifications in the computational procedures have also been carried out. The software simulation tools have been developed using Mathworks Matlab software.

The rest of the paper is organized as follows: in Section 2, we discuss recent literature on DBA for EPONs, Section 3 describe the algorithms to be compared, Sections 4 and 5 contain the results and discussion. We end with some conclusions and explain some future works.

II. STATE OF ART

There are research papers that apply techniques for DBA in EPON networks. In [3], the authors examine Passive Optical Networks (PON) architectures and DBA algorithms. The main branches of their classification for DBA methods are: grant sizing, grant scheduling, and optical network unit queue scheduling. They examine the topics of QoS support, as well as fair bandwidth allocation. The results are summarized and explicitly point to posible future avenues of research. In [4], an enhanced QoS-based dynamic bandwidth allocation (EQDBA) mechanism is proposed which incorporates with a prediction-based fair excessive bandwidth allocation (PFEBA) scheme to support differential traffic class in EPON. The proposed EQDBA mechanism divides a frame into two parts; one is the high priority traffic, which is always assigned in the fixed location of the frame to minimize the delay variation. The other kind of traffic, to solve the idle period problem, is dynamically adjusted in the transmission order according to an unstable degree list. The simulation results show that the proposed mechanism outperforms the PFEBA and QDBA mechanisms in terms of average end-to-end delay and high priority traffic delay to ensure QoS. In [6], the authors present a survey of the state of the art DBA algorithms for EPONs. They explain the main concepts and issues related to DBA in EPON systems. This paper justifies why IPACT, CCT and SBAHPS are the most suitable DBA algorithms. In [7], the authors show the differences between EPON and GPON (such as: bandwidth utilization, delay, and jitter) by means of simulations for the two standards. They take into account the evolution of both technologies to their next-generation counterparts with a bit rate of 10 Gbps and analyze the implications for the DBA. The authors propose a new GPON DBA method to study the GPON performance. It is shown that the length of the polling cycle is a key issue for the DBA within the two standards. Minor differences regarding DBA for current and next-generation PONs were also detected. In [12], the author emulates a 10Gbps next generation EPON network, which transmits voice, video and data packets, using the DBA-MAX, DBA-LINEAR and DBA-GATED algorithms. The performance is compared studying the variations of the average delay and the throughput with the traffic load. In [11], the authors provide a classification and a detailed comparison for a large number of DBA algorithms with respect to time delay and throughput parameters as performance indicators. The study explains that IPACT WITH CBR, UDBA, IPACT with two stages and CPBA algorithms show good results.

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-554-8

There are also a few studies regarding IPACT and its variances. Some of them are:

- [8], where the authors propose a new DBA algorithm. The method provides constant and predictable average packet delay and minimizes the delay variation for the high and medium priority traffic, keeping the packet loss rate under control.
- [9], where the authors describe an improved weighted interleaved polling with adaptive cycle time (IW-IPACT) algorithm according to the QoS requirement for different kinds of traffic. Strict priority scheduling was applied to the expedited forwarding services and, the weighted fair queuing scheduling was used for the rest of the services.
- [10], where the authors present a dynamic bandwidth allocation model. They propose a local bandwidth allocation algorithm based on a bargain—bargain approach. Reordering the delivery date of each packet after bargaining it according to its user level, delay and size. The model improves the traditional IPACT algorithm which establishes the delivery date of each packet in the order of polling. The results show that the proposed model can effectively minimize the Unused Slot Remainder (USR), and improves bandwidth allocation efficiency.

As a novelty, we analyze the CCT algorithm, and carry out specific variations in the SBAHPS and IPACT methods. We also study among other parameters: the average cycle times, the cycle time standard deviation and the waste of channel capacity for the high and low priority traffics. These experiments (algorithms and parameters) have been chosen because IPACT, CCT and SBAHPS algorithms are considered as the most efficient methods in the scientific bibliography, and because these parameters allow to evaluate precisely the behavior of them.

III. BANDWIDTH ALLOCATION FOR UPSTREAM DATA TRANSMISSION

This section describes the main DBA algorithms that have been simulated: IPACT, CCT and SBAHPS methods. Simulation results are presented in Section 4.

In general, the OLT allocates the size of transmission windows for each ONU using the GATE message. This allocation is based on the information received from ONUs in the REPORT message.

A. Interleaved Polling with Adaptive Cycle

The OLT polls the ONUs individually and issues grants to them in a round-robin fashion [2]. At the end of a transmission window, an ONU reports its queue sizes. The OLT employes this data to establish the next granted transmission window. The knowledge of the distance between OLT and ONUs (*d*) allows the OLT to schedule transmission windows so that packages from different ONUs do not overlap in time.

The OLT controls and allocates a transmission window for each ONU at levels below an established maximum value (*TMax*) according to the Service Level Agreement (SLA). If the transmission window requested by an ONU is lower than *TMax*, the OLT will allocate this value to the ONU. If not, the OLT will allocate *TMax* as transmission window size.

B. Constant Cycle Time

This algorithm does not carry out a sequential pool of ONUs. The transmissions from each ONUs are undertaken in a cyclical manner. Once the transmission in the cycle $TCycle_j$ is finished, each ONU will have sent a REPORT message with the request related to the transmission window for the cycle $TCycle_{j+2}$. This method ignores the requested window size from each ONU and always grants the estimated *TMax* in a cycle as window size. The main disadvantage of this algorithm is that the cycle time is not used efficiently by those ONU with little information to tranmit.

*TMax*in cycle *j+2* is defined as:

$$TMax\text{in cycle } j+2 = \sum_{k=1}^{k=N}(TCycle_{jk} - TAuto_{jk})/\mathrm{N} \qquad (1)$$

Where:

- $TCycle_j$: Time needed by the ONUs to transmit the granted length of data together with their associated guard intervals in the cycle *j*.
- *TAuto*: Time required to detect newly-connected ONUs and handle the round-trip delay and MAC address of ONUs in the cycle *j*.

  We suggest raising the efficiency in the use of resources employing the ICCT algorithm, which is based on the following premises:

  - The OLT summarizes the unused transmission window time in cycle *j* (UT_{ij}) for all ONUs with a window size lower than *TMax*, The OLT grants this calculated value($t_{re\text{-}assignedj}$) to those ONUs that have requested a window higher than *TMax* (P_j).

  $$t_{re-assignedj} = \frac{\sum_{i=1}^{N}(UT_{ij})}{P_j} \qquad (2)$$

  - In the event that all ONUs request a window size higher than *TMax*., the allocations are equitably distributed in a manner similar to the CCT algorithm.

C. Static Bandwidth Allocation for High Priority Services

In relation to the SBAHPS method, based on the investigation [5], we suggest prioritizing delay-sensitive traffic (IP telephony, video-streaming, etc) by reserving a specific time slot. This time slot should be proportional to the allocated transmission window for each ONU. This procedure works similarly to the IPACT algorithm but booking a specific time slot for the high priority traffic in each ONU. However, this particular slot can be used inefficiently by an ONU has not enough traffic to fill it completely.

IV. SIMULATION OF ALGORITHMS

The simulation environment should be suitable for the most usual applications. Its requirements are:

- EPON network with bidirectional 1 Gbps links ($C = 10^9$ bits/second) using 1490 nm wavelength for downstream and 1310 nm for upstream, with 1550 nm reserved for additional services. This network has a 1:32 split ratio.
- ONUs are located at a distance of *d* km from the OLT.
- The network is in a stable condition at the simulation time.
- The network should be characterized by the parameters indicated below, where:
- *N* is the total number of ONUs.
- *M* is the total number of ONUs transmiting low priority data traffic.
- Each ONU(*i)* processes data traffic according to a Poisson distribution, which has a mean arrival rate of λ_i packages every second. A package requires a mean service time*E(X)*. ONU*i* has a traffic load ρ_i.

$$E(X) = \frac{1}{\mu} = 8 . \frac{1518}{10^9} = 12.14\, \mu seg \quad (3)$$

$$\rho_i = \frac{\lambda_i}{\mu}; \; i=1:N \quad (4)$$

- The OLT processes a total traffic load ρ_{Total}

$$\rho_{Total} = \sum_{i=1}^{N} \rho_i \leq 1 \quad (5)$$

$$\rho_i \in [0\,, 1] \qquad \rho_i = \rho_i^{HP} + \rho_i^{LP} \quad (6)$$

$$\rho_{total} = \sum_{i=1}^{N} \rho_i = \sum_{i=1}^{N} (\rho_i^{HP} + \rho_i^{LP}) \leq 1 \quad (7)$$

- ρ_i^{HP} is the traffic load for packages related to high priority services (percentage of ρ_i).
- ρ_i^{LP} is the traffic load for pakages related to low priority services (percentage of ρ_i).
- For one ONU *i*, a cycle time *j*, T*Cycle*$_j$, represents the elapsed time between transmission start times *j+1* and *j*.
- The average cycle time, E(*TCycle*^{HP}*)*, for the packages related to high priority servicesis defined as:

$$\text{E}(TCycle^{HP)} = \frac{N.\ TCycle_0}{1-\rho} \quad (8)$$

- The average cycle time, E(*TCycle*^{LP}), for the packages related to low priority services is defined as:

$$\text{E}(TCycle^{LP}) = \frac{N}{M} \frac{N.\ TCycle_0}{1-\rho} \quad (9)$$

- The waste of channel capacity in the cycle *j*, *WCj(%),* is defined as:

$$WCj(\%) = TCycle_{jwasted} / TCycle_j \;.\, 100 \quad (10)$$

- The waste of channel capacity for the high priority services in the cycle *j*, *WCj*^{HP}*(%)*, is defined as:

$$WCj^{HP}(\%) = TCycle_{jwasted}^{HP} / TCyclej^{HP} \;.\, 100 \quad (11)$$

- ρ_{Total} will have the values: 0.1, 0.3, 0.5, 0.7, 0.9.
- ρ_i^{HP} (percentage of ρi) will have the values: 0.1, 0.3, 0.5, 0.7, 0.9.

$$\text{E}(TCycle) = \frac{1}{\mu} \cdot \lambda \cdot E(TSim) + N \cdot E(TGuard\ \ ) + N \cdot E(TRep\ \ ) \quad (12)$$

$E(TSim)$ *is the* average time for the execution of the simulation scenario.

$E(TGuard)$ is the average guard time. (13)

$E(TRep)$ is the average required time for the transmission of the REPORT message (64 bytes).
TReq$_i$ is the requested transmission window.

$$TRep = \frac{\rho_{Total}}{N} \quad (14)$$

$$TReq_i = TCycle_0 + \frac{1}{\mu} NPaq_i \quad (15)$$

N_{paq_i} is the number of packages that ONU$_i$ asks to transmit.

A. Interleaved Polling with Adaptive Cycle

Below, we explain the main simulation environments and the obtained results for the IPACT algorithm.

TABLE I. PARAMETERS USED IN THE IPACT ALGORITHM SIMULATION

N	*M*	ρ^{HP}
4	4	0.3

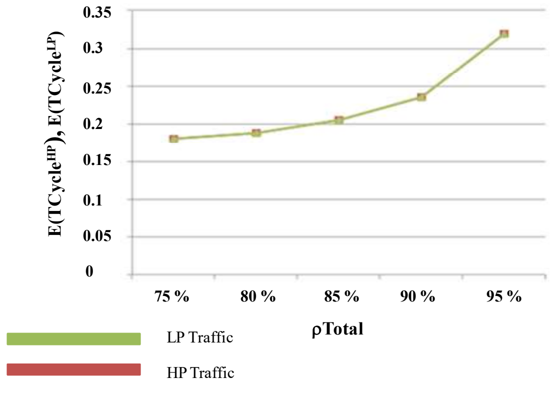


Figure 1. IPAC algorithm: E(TCycle^{HP}), E(TCycle^{LP}) in microseconds as a function of ρTotal forρ^{HP} = 0.3 [1].

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-554-8

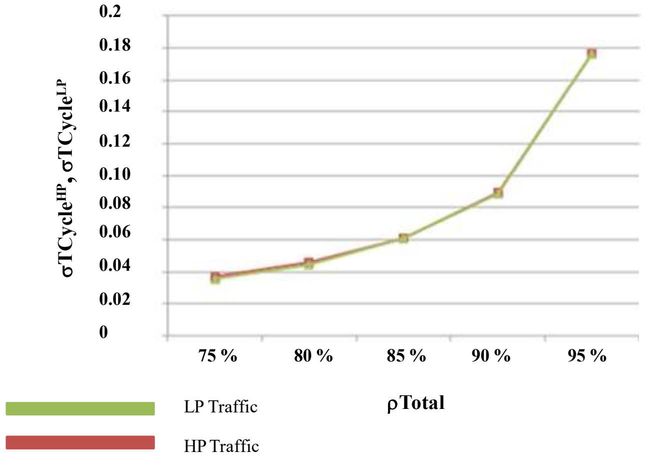


Figure 2. IPAC algorithm σTCycle^{HP}, σTCycle^{LP}in microseconds as a function of ρTotal for ρ^{HP} = 0.3 [1].

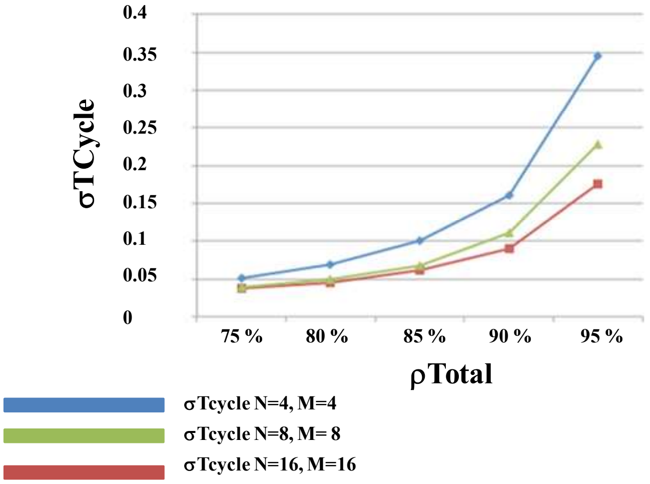


Figure 3. IPAC algorithm: σTCycle in microseconds as a function of ρTotal with ρ^{HP} = 0.3 for several values of N and M [1].

Figure 1 shows that there is not a clear distinction between the average cycle times for high and low priority traffic when the relation between *N* and *M* parameters is 1. Figure 2 shows the progressive growth of the cycle time standard deviation when the total traffic, ρ_{Total}, increases. Figure 3 displays how the cycle time standard deviation increases as the number of ONUs raises, this fact is particularly relevant for high traffic demands (i.e., in ρ_{Total} = 95% , $(\sigma\left(T_{ciclo}^{N,M=16}\right) \approx 2 \cdot \sigma(T_{ciclo}^{N,M=4}))$.

The results show that IPACT algorithm carries out an efficient use of resources; however, is very sensitive to fast traffic changes or unstable traffic flows.

B. *Constant Cycle Time*

Below, we describe the main simulation environments and the obtained results for the CCT algorithm.

TABLE II. PARAMETERS USED IN THE CCT ALGORITHM SIMULATION

N	*M*	*ρHP*	*TMax (msecond)*
4	4	0.1	0.05

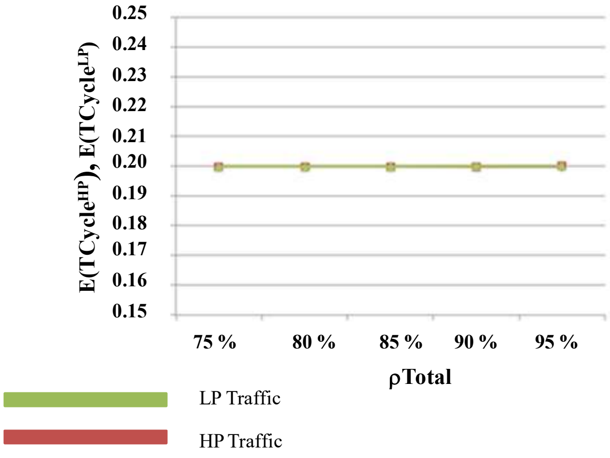


Figure 4. CCT algorithm: E(TCycle^{HP}), *E(TCycle^{LP})* as a function of ρ_{Total} for *N*= 4, *M*= 4,ρ^{HP} = 0.1 and *TMax* = 0.05 [1].

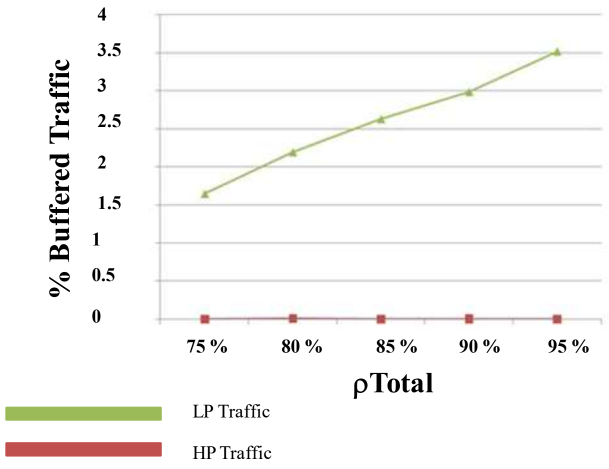


Figure 5. CCT algorithm: % Buffered HP and LP traffic as a function of ρ_{Total} for *N*= 4, *M*= 4, with ρ^{HP} = 0.1 and *TMax* = 0.05 [1].

Figure 4 shows that the algorithm works properly, since it allocates a constant cycle time for each simulation scenario.Several values for ρ_{Total} are tested.

In Figure 5, it can be noted that the package prioritization works properly as the traffic load (ρ_{Total}) increases –even if the low priority traffic data stored in the buffer increases.

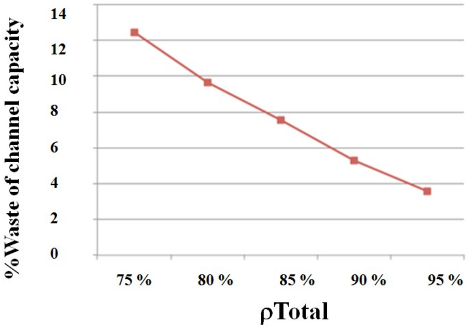


Figure 6. ICCT algorithm: Waste of channel capacity as a function of ρ_{Total} for N= 4, M= 4, with ρ^{HP} = 0.1 and $TMax$ = 0.05 [1].

Figure 6 shows that there is not a significant waste of the channel capacity and its value decreases as ρ_{Total} grows. The same pattern with very slight variations in the value of the waste has been observed for ρHP = 0.3, 0.5, 0.7 and 0.9.

TABLE III. PARAMETERS USED IN THE ICCT ALGORITHM SIMULATION

N	*M*	ρ^{HP}	*TMax(msecond)*
4	4	0.1	0.05

In Figures 7, 8, and 9, it can be noted that the algorithm works properly, the high priority traffic is adequately prioritized and there is no waste in the allocated time. However, the low traffic data stored in the buffer increases as the total traffic load raises, although lower in magnitude than in the CCT algorithm. Figure 10 shows the average cycle time for several values of M and ρ^{HP} = 0.1. It should be noted that a decrease in the number of ONUs transmitting low priority data traffic implies a considerable increase in the average cycle time for this kind of traffic. Figure 11 shows that the low traffic stored in the buffer increases as the total load traffic grows for all M values.

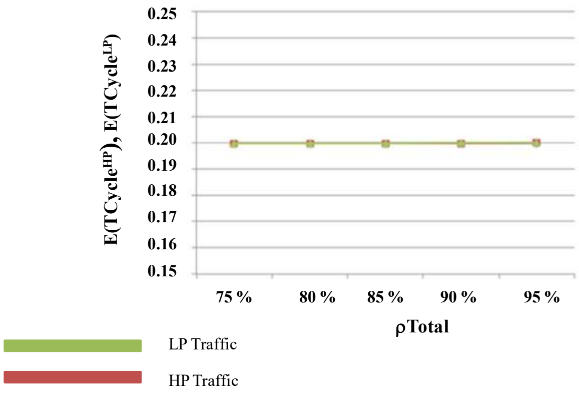


Figure 7. ICCT algorithm: E(TCycle^{HP}), E(TCycle^{LP}) in microseconds as a function of ρ_{Total} with ρ^{HP} = 0.1 [1].

The results show that ICCT method prioritizes the high priority traffic with an insignificant impact on the low priority traffic delay. However, the low priority traffic stored in the buffer increases as the total traffic flow grows.

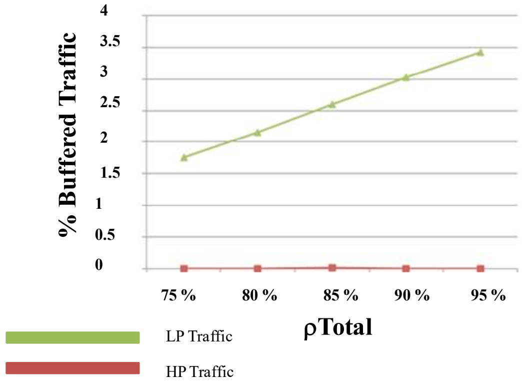


Figure 8. ICCT algorithm: Buffered HP and LP traffic as a functionρ_{Total} for ρ^{HP} = 0.1 [1].

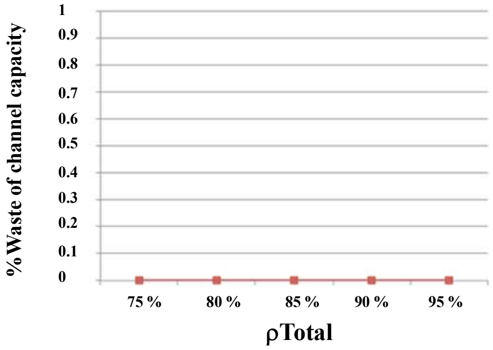


Figure 9. ICCT algorithm: Waste of channel capacity as a function of as a function of ρ_{Total} for N= 4, M= 4, ρ^{HP}= 0.5, TR = 0.2 and $TMax$ = 0.05 [1].

C. Static Bandwidth Allocation for High Priority Services (SBAHPS)

Below, we explain the main simulation environments and the obtained results for the SBAHPS algorithm.

TABLE IV. PARAMETERS USED IN THE SBAHPS ALGORITHM SIMULATION

N	*M*	ρ^{HP}	*TR*	*TMax (msecond)*
4	4	0.5	0.2	0.05

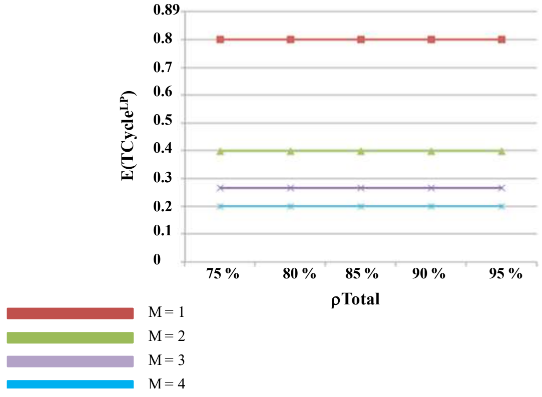


Figure 10. ICCT algorithm: E(TCycleLP) in microseconds as a function of ρ_{Total} for several values of M, , HP = 0.1 and TMax = 0.05 [1].

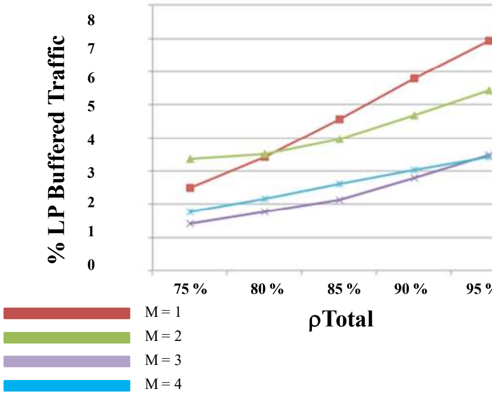


Figure 11. *ICCT: algorithm: %Buffered LP traffic* as a function of ρ_{Total} for *several values of M,* , ρ^{HP} = 0.1 and *TMax* = 0.05 [1].

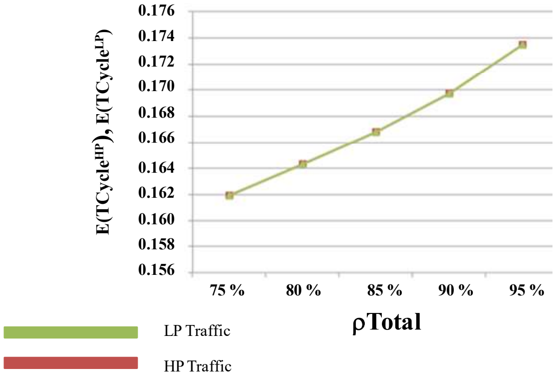


Figure 12. SBAHPS algorithm: *E(TCycle^{HP}), E(TCycle^{LP})*in microseconds as a function of ρ_{Total} for *N*= 4, *M*= 4, ρ^{HP}= 0.5, *TR* = 0.2 and*TMax* = 0.05 [1].

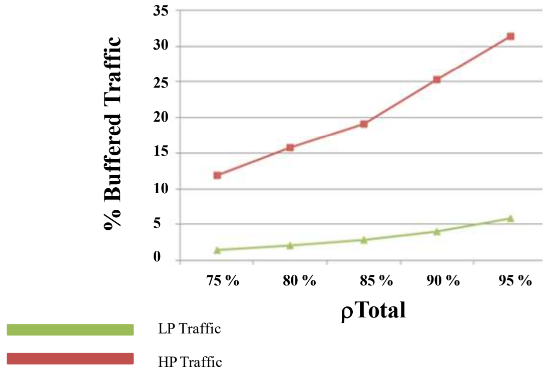


Figure 13. SBAHPS algorithm: % Buffered HP and LP traffic as a function of ρ_{Total} for *N*= 4, *M*= 4, ρ^{HP}= 0.5, *TR* = 0.2 and *TMax* = 0.05 [1].

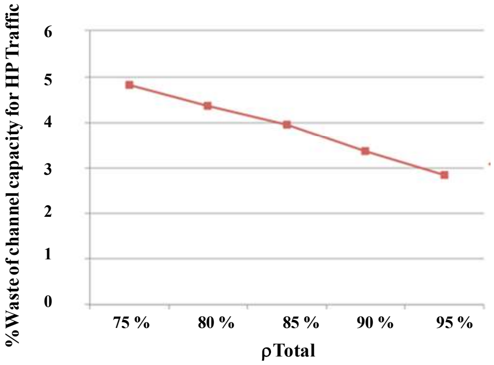


Figure 14. SBAHPS algorithm: Waste of channel capacity as a function of ρ_{Total} for*N*= 4, *M*= 4, ρ^{HP}= 0.5, *TR* = 0.2 and *TMax* = 0.05 [1].

Figure 12 shows that the growth of the average cycle time is connected to the increase of the total traffic load. In Figures 13 and 14, it can be noted that the high priority data traffic stored in the buffer is much higher than the low priority traffic. There is not a significant waste of reserved capacity. This waste is slightly decreased if the total traffic increases.

The results show that the SBAHPS algorithm gets suitable constant cycle times and low priority buffered traffic flows. However, it has an inefficient bandwidth usage for the high priority traffic.

V. CONCLUSIONS AND FUTURE WORKS

We have analyzed the main algorithms utilized for the bandwidth allocation in EPON: IPACT, CCT and SBAHPS methods. Several computer simulations were carried out to reproduce the behavior of these algorithms and study their characteristics.

IPACT algorithm could be easily implemented and showed a good performance. However, due to the impact on the time-length cycle variations, caused by requests of big transmission windows from any ONU, it was difficult to achieve a minimum guarantee quality service when a specific delay was required (audio streaming, VoIP, video conference, etc.). The ICCT algorithm, which we use instead of the CCT method to raise the efficiency in the use of resources, had an important computational complexity. However, its capability to assign unused capacity intransmission windows, caused that the resources were more efficiently used for the data transmission upstream. The SBAHPS algorithm booked a transmission time for the high priority traffic, which was proportional to the allocated window for the rest of traffic. The control performed with the aim of limiting the maximum transmission window in each ONU, allowed to guarantee a QoS. Additionally, its configuration could be adapted to work in a similar way to IPACT and ICCT algorithms.

Our future research will build a proof of concept based on the simulation, which will test several real scenarios.

REFERENCES

[1] J. A. Infantes, Master's Final Project: Estudio de Viabilidad de Algoritmos de Asignación de Ancho de Banda en Canal Ascendente sobre Redes EPONwith D. Larrabeiti as tutor and M.L. Mouronte as director, Universidad Carlos III de Madrid, 2013.

[2] G. Kramer, B. Mukherjee, and G. Pesavento, "IPACT: A Dynamic Protocol for an Ethernet PON (EPON)", IEEE Communications Magazine, vol. 40, no. 2, pp. 74-80, 2002.

[3] M. Mcgarry, M. Reisslein, and M. Maier, "Ethernet Passive Optical Network Architectures and Dynamic Bandwidth Allocation algorithms", IEEE communications surveys and Tutorials, vol. 10, no.3, pp. 46-60, 2008.

[4] I.S. Hwang, Z. D. Shyu,and J. Y. Lee., "*A QoS-Enhanced Dynamic Bandwidth Allocation Mechanism in EPONs",*Journal of Computational Information Systems, vol. 6 ,no. 11, pp. 3527-3533, 2010.

[5] I. T. Orphanoudakis et al., "Efficient resource allocation with service guarantees in passive optical networks", Journal of Optical Networking, vol. 6, no. 7, pp.884-896, 2007.

[6] J. Zheng and H. T. Mouftah, "A survey of dynamic bandwidth allocation algorithms for Ethernet Passive Optical Networks, Optical Switching and Networking", vol. 6, no. 3, pp. 151-162, 2009.

[7] B. Skubic, J. Chen, J. Ahmed, L. Wosinska, and B. Mukherjee, "A Comparison of Dynamic Bandwidth Allocation for EPON, GPON, and Next-Generation TDM PON", IEEE Communications Magazine, vol. 47, no. 3, pp. S40 - S48, 2009.

[8] A. Dixit, B. Lannoo, G. Das, D. Colle, M. Pickavet, and P.Demeester, "Dynamic Bandwidth Allocation with SLA Awareness for QoS in Ethernet Passive Optical Networks", J. Opt. Commun. Netw, 2013, pp.1-14. [Online]. Available from: https://biblio.ugent.be/publication/3262566/file/3262574.

[9] F. Xiao, Z. Zhang, and X. Yin, "An Improved Weighted IPACT Algorithm of EPONs in Smart Distribution Networks Based on the Requirements of Relay Protection", International Transactions on Electrical Energy Systems, 2016, vol. 26, no. 10, pp. 2107–2122.

[10] G. LU and J. W. QI, "A Model Based on Multi-agent for Dynamic Bandwidth Allocation in Networks", 2016 Joint International Conference on Artificial Intelligence and Computer Engineering (AICE 2016) and International Conference on Network and Communication Security (NCS 2016), ISBN: 978-1-60595-362-5. . [Online]. Available from: http://dpi-proceedings.com/index.php/dtcse/article/viewFile/5697/5315.

[11] A. Mohammed, M. A. Maher, M. H. Aly, "EPON Performance Optimization: An Extensive Comparative Study for DBA Algorithms", Optoelectronics and Advanced Materials-Rapid Communications, vol. 10, no. 7-8, pp. 503-508, 2016.

[12] S. P. Rout, "Performance Comparison of Various DBA Algorithms on an Emulated 10Gbps Next Generation EPON Access Network, International Journal of Innovative Research in Computer and Communication Engineering", vol. 4, no. 5, 2016, pp. 9377-9382. [Online]. Available from: . https://www.ijircce.com/upload/2016/may/183_50_Performance.pdf

A Novel Passive Tracking Scheme Exploiting Adaptive Line of Sight Links

Deockhyeon Ahn, Jungpyo Lee, Chao Sun, Youngok Kim*
Electronic Engineering Dept.
Kwangwoon University
Seoul, Republic of Korea
e-mail: *kimyoungok@kw.ac.kr

***Abstract*—The wide deployment of wireless access points and smart mobile devices has been recently addressed in the research field of positioning. In traditional positioning schemes, the target is assumed to hold a tag or a transceiver for being tracked and it is regarded as active tracking. However, the target without any tags nor transceivers can be tracked by using radio frequency tomography, and it is known as passive tracking. In this paper, we propose a passive tracking scheme exploiting adaptive line-of-sight links (LOSLs). In the proposed scheme, the LOSL between each of wireless mobile device and wireless access point can be constructed adaptively to enhance the tracking performance in indoor environment. It maintains only least links while waiting for detection of a target with minimum energy consumption. However, when a target is detected with the least links, we can get a more accurate trajectory of the target by adaptively increasing the complexity of the links higher. According to the simulation results, it is shown that the proposed scheme can enhance the positioning performance remarkably.**

Keywords-positioning; active tracking; passive tracking; adaptive links.

I. INTRODUCTION

According to literatures, positioning schemes can be classified into two categories: Active tracking that requires the target to hold actively a device for tracking, such as a tag or a transceiver, and Passive tracking that tracks passively the target without any of devices [1]. However, the active tracking scheme has a limitation that it is not always expected for the tracked persons, such as criminals and intruders, to possess any devices for tracking. Accordingly, this issue has provoked much research about the passive tracking scheme. Zhou et al. had introduced a passive indoor tracking scheme with geometrical formulation [2]. They explored the characteristics of the wireless propagation radio frequency tomography (RFT) [3]-[6], under line-of-sight links (LOSLs), and by formulating the geometrical problem and applying Particle Swarm Algorithm (PSO) [7], the trajectory of the target can be estimated accurately. However, it is not efficient to maintain complex LOSLs under waiting for detection of a target with energy consumption. Moreover, since there are limitations of detecting multi-targets and more complex situations with triggered sequence error or time stamp error. In this paper, we propose a novel passive tracking scheme exploiting adaptive LOSLs to overcome the limitations of the conventional scheme. Therefore, we can get a more accurate trajectory of the target by increasing adaptively the level of the link complexity higher, while the conventional scheme is based on the fixed LOSLs.

The rest of the paper is organized as follows. In Sect. II, the basic concept of the conventional passive tracking scheme based on RFT are briefly discussed. In Sect. III, a passive tracking scheme exploiting adaptive LOSLs is proposed. In Sect. IV, the positioning performance of the proposed scheme is evaluated with computer simulations. Finally, our concluded remarks are summarized in Sect. V.

II. SYSTEM DESCRIPTION

A basic concept of the conventional passive tracking scheme based on RFT is described in Figure 1. As shown in the figure, a RFT operator consists of two access points (APs) (1, 2) and two RSS indicators (a, b), and it estimates a cross point (CP) on the LOSL [2]. Note that the CP indicates the intersecting point by the target on the LOSL. Both the RSS Indicators and the APs are placed on either side of the corridor, forming a LOSL web to monitor the corridor. When an obvious RSS fluctuation on a LOSL is detected, it is defined as this LOSL is triggered by the target. When a pedestrian walks across the RFT operator from position A to B in Figure 1, the triggered sequence of LOSLs is record as L(i), (i = 1, 2, 3, 4), which are L(1, a), L(1, b), L(2, a), and L(2, b), respectively. Note that L(i) is represented as a 1st order straight line, $y = k_i \cdot x + b_i$, where k_i and b_i are foreknown according to the coordinates of the APs and the RSS Indicators.

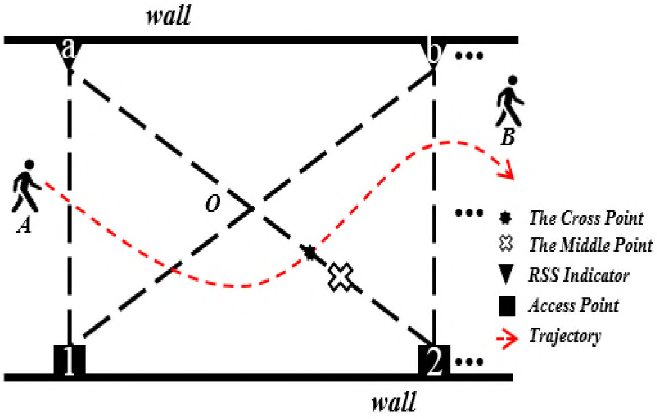
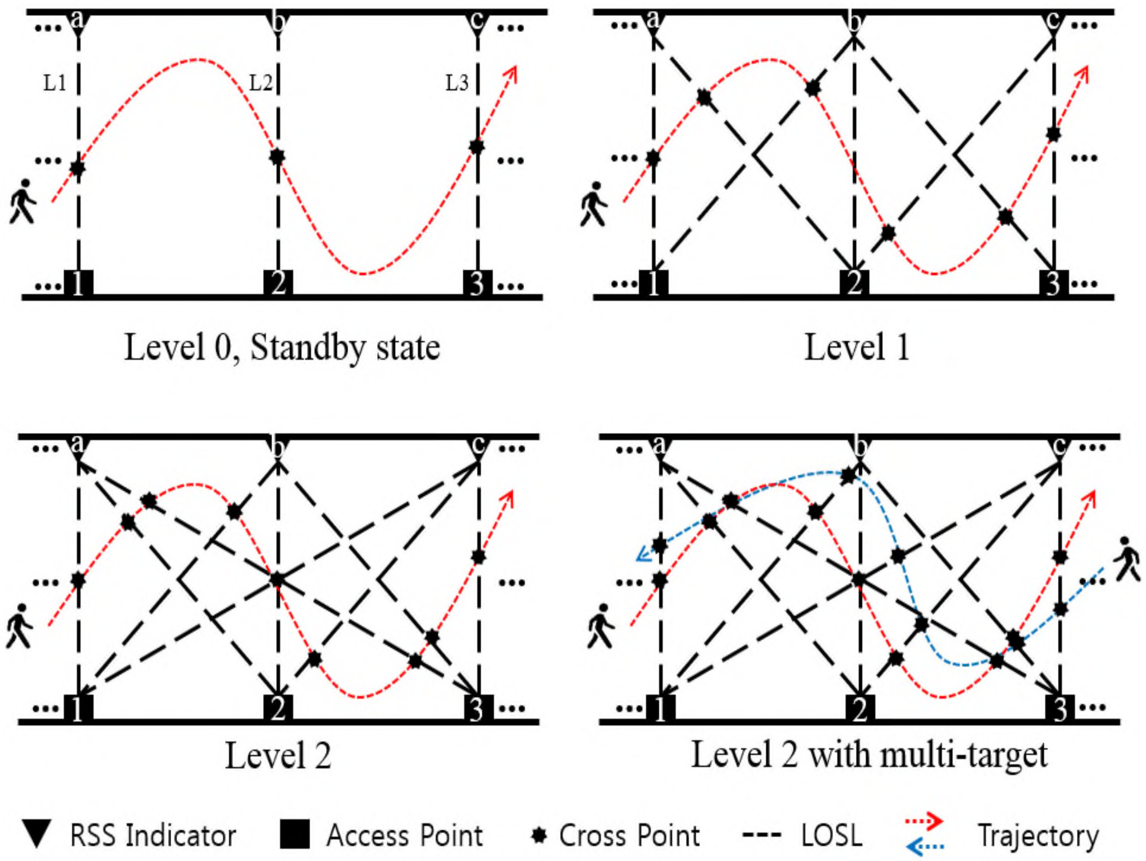


Figure 1 . CP estimation on L(2,a) by a RFT operator



Level 0, Standby state

Level 1

Level 2

Level 2 with multi-target

Figure 2. Scenario with proposed scheme

Generally, when L(i) is triggered, the middle point, which is *O* on L(3) in Figure 1, on L(i) is selected as the CP for minimizing the tracking error, and it is called as a central method (CM) scheme. Once the triggered sequence is considered, however, the CP can be set as the middle point of the restricted segment (the cross mark in Figure 1) on the LOSL, which is cut by the previous obstructed LOSL and the subsequent obstructed LOSL, and it is given as follows:

$$x_{cp}^{i}, y_{cp}^{i} \in [the\ segment\ on\ LOSL(i)\ cut\ by\ LOSL(i-1)\ and\ LOSL(i+1)] \quad (1)$$

For example, in Figure 1, the CP on L(2, a), must locate on segment *O*2 in common sense because the previous triggered LOSP is L(1, b) and the later triggered LOSP is L(2, b). However, if the previous triggered LOSP is L(1, a) and the later triggered LOSP is L(2, a), the CP will be located on segment *O*a. With the presented example in Figure 1, therefore, the CP is located at the middle point of segment *O*2, which is cut by L(1, b) and L(2,b) for further minimizing the tracking error.

III. PROPOSED SCHEME

As for the conventional scheme, it is not efficient to maintain complex LOSLs under waiting for detection of a target with energy consumption. We assumed that more transmitting power is used to maintain complex links, because the distance between AP and RSS indicator is increased. Moreover, there are other limitations of detecting multi-targets and performance with fixed structure of LOSL web. In this paper, therefore, we propose a novel passive tracking scheme exploiting adaptive LOSLs.

Figure 2 shows a scenario with the proposed scheme. In the proposed scheme, it remains level 0, as the standby state with minimum number of LOSLs. When the LOSL is triggered, the level is changed to higher level with respect to the situations such as multi-targets or enhanced accuracy of tracking. In this paper, three representative situations are considered; when we want to get higher accuracy of the trajectory of the target, when the multi-targets are detected, when the sequence history of trajectory of the target is not clear.

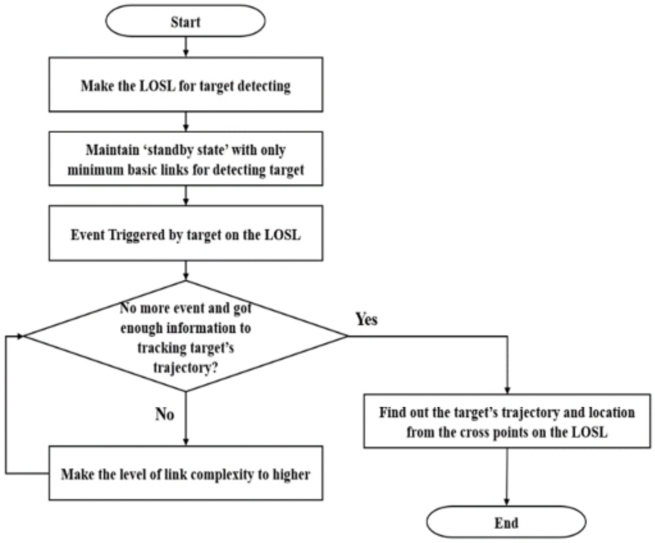

Start
Make the LOSL for target detecting
Maintain 'standby state' with only minimum basic links for detecting target
Event Triggered by target on the LOSL
No more event and got enough information to tracking target's trajectory?
Yes
No
Find out the target's trajectory and location from the cross points on the LOSL
Make the level of link complexity to higher
End

Figure 3. The flow chart of proposed scheme

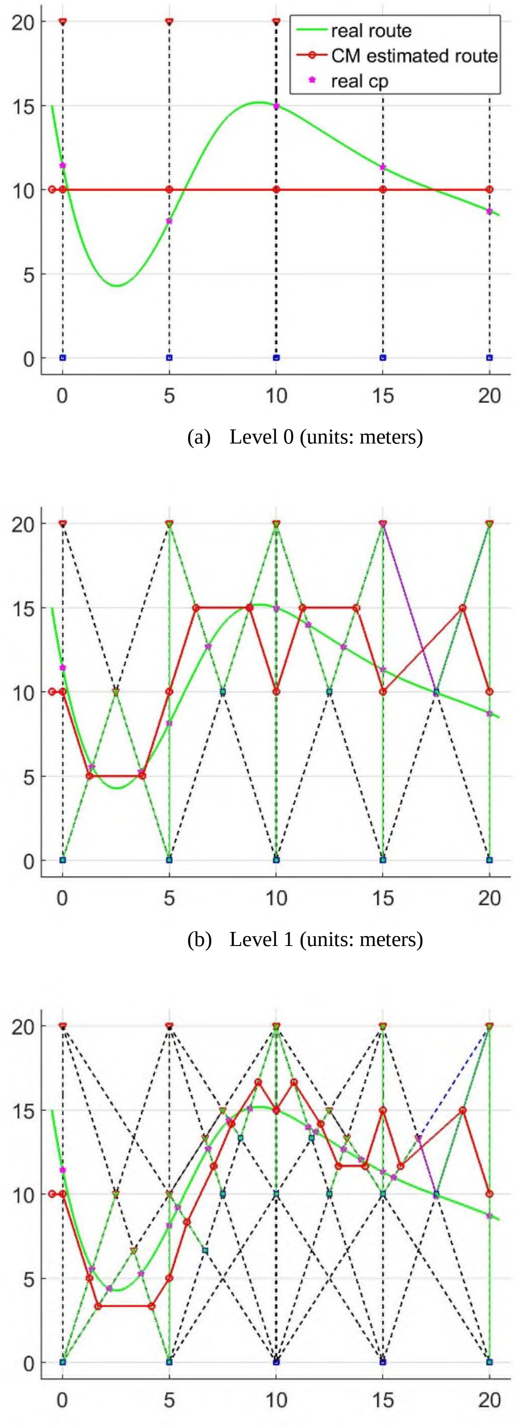
Firstly, when we just want to get higher accuracy, we can make it by increasing the number LOSLs per each of nodes as shown in the Figure 2. By changing level 0 to 2, then, we can get more CPs, and we can track the trajectory of the target more densely.

Secondly, if we get different trigger sequences with different directions, compared with originally tracked trajectory, then we can assume that there are multiple targets. Tracking of the multi-targets cannot be achieved with only the low levels. To make a clear division with original target, we can increase the number of LOSLs and compare the triggered sequence of original target with that of new targets. Moreover, by increasing the number of LOSLs, we can decrease the tracking error when the sequence history of trajectory of the target is not clear.

Figure 3 presents the flow chart of the proposed scheme. For the first step, we make the LOSLs for target detection by sending propagation signals from APs to RSS Indicators. Then, it maintains 'standby state' with only minimum basic links for detecting target while saving power consumption. When a target is detected with the basic links, the proposed scheme increases the complexity of LOSL. Meanwhile, if the proposed scheme has enough information of the sequence with time stamp for tracking the target, it moves on to the next step to find out the trajectory of the target. However, if the information of the sequence with time stamp is missed or the sequence history is not reasonable, then it moves on the next step. In the next step, it can bring the level of LOSL to higher level and goes back to former step until the conditions are satisfied.

IV. PERFORMANCE EVALUATION

We performed computer simulations with MATLAB. In the simulations, Wi-Fi APs and smart-phones are assumed as APs and RSS indicators, and the characteristics of Wi-Fi signal are measured and modeled with path-loss and fading effects. The simulation also models a 20m x 20m space with 5 APs and 5 RSS indicators to validate the effectiveness of the proposed scheme.



(a) Level 0 (units: meters)

(b) Level 1 (units: meters)

(c) Level 2 (units: meters)

Figure 4. Results of simulations with the proposed scheme (x-axis and y-axis indicate the coordinates in meters)

With the proposed scheme, we used the CM scheme, which sets the central point of each of the LOSLs to the CP for estimating the real CP, which is the intersecting point by the target on the LOSL. Note that purple stars indicate the real CPs on the actual trajectory of target. Figure 4 shows the result of simulations with the proposed scheme. The green solid line indicates the actual trajectory of target, which is made randomly, while the red line with circle marks indicates the estimated trajectory of the target and the dotted lines are the LOSLs. As shown in the figure, the proposed scheme can change the levels of LOSL web from 0 to 2 and even more to enhance the tracking performance. Note that the level 1 is the tracking performance with the conventional scheme. In the simulations, we used only five couples of APs, but we can notice that the performance of tracking is enhanced remarkably, and the errors are reduced as the number of LOSLs is increased. It is reasonable that the power consumption of the proposed scheme is decreased because it can save the transmitting power, while it waits for the target. However, the amount of power saving depends on the scenarios with different ratio of waiting time and active time. Therefore, we are under performing experiments for the proposed scheme to confirm the operation of the algorithm in terms of the power saving as well as the accuracy, and the results will be discussed in future works. Moreover, if there is an error of the triggered sequence or time stamp, which is caused from events of the multi-targets, the proposed scheme can track the multi-targets with independent sequence and time stamp.

V. CONCLUSIONS

In this paper, we proposed a passive tracking scheme exploiting adaptive LOSLs. In the proposed scheme, the LOSL between each of wireless mobile device and wireless APs can be constructed adaptively to enhance the tracking performance in indoor environment. Compared with the conventional scheme, we can get advantages in accuracy, while maintaining the existing number of APs, by increasing the number of LOSLs in each of levels. It is natural that the tracking accuracy becomes higher when the number of APs increases. However, there are several issues left for future works. As the number of LOSLs is increased, the complexity also is proportionally increased. Therefore, one of the future work is to find an optimal number of APs' deployment for tracking a target in usual indoor environment. Also, we need to evaluate the performance of the proposed scheme with various number of multi-targets in future works. Moreover, we will analyse the stability of the algorithm with respect to the accuracy of the inputs in future works.

ACKNOWLEDGMENT

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the ministry of Education (NRF-2016R1D1A1B03932980).

REFERENCES

[1] G. Deak, K. Curran, and J. Condell, “A survey of active and passive indoor localisation systems,” *Comput. Commun.*, vol. 35, pp. 1939–1954, Sep. 2012

[2] B. Zhou, N. Kim, and Y. Kim, "A Passive Indoor Tracking Scheme With Geometrical Formulation," *IEEE Antennas and Wireless Propagation Letters*, vol. 15, pp. 1815-1818, Oct. 2016.

[3] S. Nannuru, Y. Li, Y. Zeng, M. Coates, and B. Yang, “Radio-frequency tomography for passive indoor multitarget tracking,” *IEEE Trans. Mobile Comput.*, vol. 12, pp. 2322–2333, Dec. 2013.

[4] Y. Guo, K. Huang, N. Jiang, X. Guo, Y. Ki, and G. Wnag, “An exponential-rayleigh model for RSS-based device-free localization and tracking,” *IEEE Trans. Mobile Comput.*, vol.14, pp. 484 - 494, Mar. 2015.

[5] O. Kaltiokallio, M. Bocca, and N. Patwari, “A fade level-based spatial model for radio tomographic imaging,” *IEEE Trans. Mobile Comput.*, vol. 13, pp. 1159–1172, Jun. 2014.

[6] I. Sabek, M. Youssef, and A. Vasilakos, “ACE: an accurate and eficient multi-entity device-free WLAN localization system,” *IEEE Trans. Mobile Comput.*, vol. 14, pp. 261–273, Feb. 2015.

[7] S. Selleri, M. Mussetta, P. Pirinoli, R. Zich, and L. Matekovits, “Some insight over new variations of the particle swarm optimization method,” *IEEE Antennas Wireless Propag. Lett.*, vol. 5, pp. 235–238, Dec. 2006.

Load Experiment of the vDACS Scheme to Use between Plural Organizations for Applications to the Small and Medium Size Scale Organization

Kazuya Odagiri
Sugiyama Jogakuen University
Aichi, Japan
e-mail: kodagiri@sugiyama-u.ac.jp,
kazuodagiri@yahoo.co.jp

Shogo Shimizu
Gakushuin Women's College
Tokyo, Japan
e-mail: shogo.shimizu@gakushuin.ac.jp

Naohiro Ishii
Aichi Institute of Technology
Aichi, Japan
e-mail: ishii@aitech.ac.jp

Makoto Takizawa
Hosei University
Tokyo, Japan
e-mail: makoto.takizawa@computer.org

***Abstract*- In the current Internet system, there are many problems using anonymity of the network communication such as personal information leaks and crimes using the Internet system. This is why TCP/IP protocol used in Internet system does not have the user identification information on the communication data, and it is difficult to supervise the user performing the above acts immediately. As a study for solving the problem such as the personal information leaks, there is the study of Policy Based Network Management (PBNM). This is the scheme for managing a whole Local Area Network (LAN) through communication control by a user unit. In the PBNM, two types of schemes exist. The first is the scheme for managing the whole LAN by locating the communication control mechanisms on the path between network servers and clients. The second is the scheme of managing the whole LAN by locating the communication control mechanisms on clients. As the scheme to control on a client, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme. By applying this DACS Scheme to Internet system management, we will realize the policy-based Internet system management. In this paper, as the progression phase for the last goal, we perform the load experiment of the cloud type virtual PBNM named the vDACS Scheme, which can be used by plural organizations, for applications to the small and medium size scale organization.**

Keywords- policy-based netwok management; DACS Scheme; NAPT

I. INTRODUCTION

In the current Internet system, there are many problems using anonymity of the network communication such as personal information leaks and crimes using the Internet system. The news of the information leak in the big company is sometimes reported through the mass media. Because TCP/IP protocol used in Internet system does not have the user identification information on the communication data, it is difficult to supervise the user performing the above acts immediately. As studies and technologies for managing Internet system realized on TCP/IP protocol, those such as Domain Name System (DNS), Routing protocol, Fire Wall (F/W) and Network address port translation (NAPT)/network address translation (NAT) are listed. However, they are the studies for managing the specific part of the Internet system, and have no purpose of managing the whole Internet system.

As a study for managing the whole Internet system for the purpose of controlling it by a user unit, the PBNM [2] exists. The PBNM is a scheme for managing a whole Local Area Network (LAN) through communication control by a user unit, and cannot be applied to the Internet system. The PBNM is often used in a scene of campus network management. In a campus network, network management is quite complicated. Because a computer management section manages only a small portion of the wide needs of the campus network, there are some user support problems. For example, when mail boxes on one server are divided and relocated to some different server machines, it is necessary for some users to update a client machine's setups. Since most of the computer network users in a campus are students and they do not check frequently their e-mail, it is difficult to make them aware of the settings update. This administrative operation is executed by means of web pages and/or posters. For the system administrator, individual technical support is a stiff part of the network management. Because the PBNM manages a whole LAN, it is easy to solve this kind of problem. In addition, the PBNM can manage a whole LAN by making anonymous communication non-anonymous. As the result, it becomes possible to identify the user who steals personal information and commits a crime swiftly and easily. Therefore, by applying the PBNM, we will study about the policy-based Internet system management.

In the existing PBNM, there are two types of schemes. The first is the scheme of managing the whole LAN by locating the communication control mechanisms on the path between network servers and clients. The second is the scheme of managing the whole LAN by locating the communication control mechanisms on clients. The client means a client

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-554-8

computer. It is difficult to apply a scheme for controlling on a network course to Internet system practically, because the communication control mechanism needs to be located on the path between network servers and clients without exception. Because the scheme for controlling on a client locates the communication control mechanisms as the software on each client, it becomes possible to apply the scheme for controlling on a client to Internet system by devising the installing mechanism so that users can install the software to the client easily.

As the scheme to control on a client, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme. As the works on the DACS Scheme, we showed the basic principle of the DACS Scheme, and security function [14]. After that, we implemented a DACS System to realize a concept of the DACS Scheme. By applying this scheme to Internet system, we will realize the policy-based Internet system management. Then, the Wide Area DACS system (wDACS system) used in one organization was showed as the second phase for the last goal. As the first step of the second phase, we showed the concept of the cloud type virtual PBNM, which could be used by plural organizations. In this paper, as the progression phase of the third phase for the last goal, we perform the load experiment to confirm the possibility of the cloud type virtual PBNM for the use in plural organizations. In Section II, motivation and related research for this study are described. In Section III, the existing DACS Scheme and wDACS Scheme is described. In Section IV, the proposed scheme and load experiment results are described.

II. MOTIVATION AND RELATED RESEARCH

In policy-based network management, there are two types of schemes. The scheme to control on a network course is the scheme described in Figure 1. The standardization of this scheme is performed in various organizations. In IETF, a framework of PBNM [2] was established. Standards about each element constituting this framework are as follows. As a model of control information stored in the server called Policy Repository, Policy Core Information model (PCIM) [3] was established. After it, PCMIe [4] was established by extending the PCIM. To describe them in the form of Lightweight Directory Access Protocol (LDAP), Policy Core LDAP Schema (PCLS) [5] was established. As a protocol to distribute the control information stored in Policy Repository or decision result from the PDP to the PEP, Common Open Policy Service (COPS) [6] was established. Based on the difference in distribution method, COPS usage for RSVP (COPS-RSVP) [7] and COPS usage for Provisioning (COPS-PR) [8] were established. RSVP is an abbreviation for Resource Reservation Protocol. The COPS-RSVP is the method as follows. After the PEP having detected the communication from a user or a client application, the PDP makes a judgmental decision for it. The decision is sent and applied to the PEP, and the PEP adds the control to it. The COPS-PR is the method of distributing the control information or decision result to the PEP before accepting the communication.

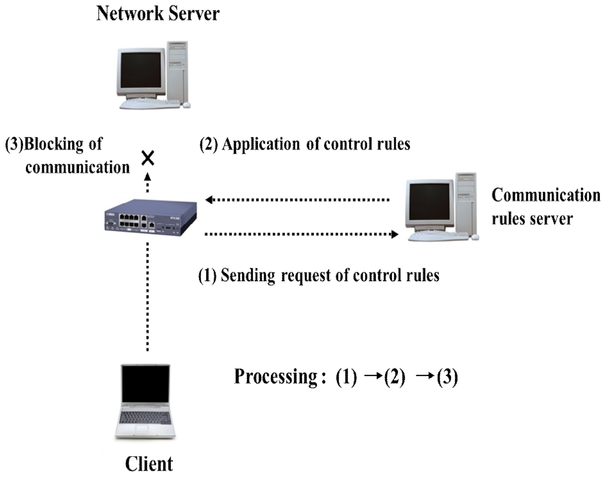

Network Server
(3)Blocking of communication
(2) Application of control rules
Communication rules server
(1) Sending request of control rules
Processing : (1) →(2) →(3)
Client

Figure 1. Principle in Scheme to Control on a Network Course

Next, in DMTF, a framework of PBNM called Directory-enabled Network (DEN) was established. Like the IETF framework, control information is stored in the server storing control information called Policy Server, which is built by using the directory service, such as LDAP [9], and is distributed to network servers and networking equipment such as switch and router. As the result, the whole LAN is managed. The model of control information used in DEN is called Common Information Model (CIM), the schema of the CIM (CIM Schema Version 2.30.0) [11] was opened. The CIM was extended to support the DEN [10], and was incorporated in the framework of DEN.

In addition, Resource and Admission Control Subsystem (RACS) [12] was established in Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN) of European Telecommunications Standards Institute (ETSI), and Resource and Admission Control Functions (RACF) was established in International Telecommunication Union Telecommunication Standardization Sector (ITU-T) [13].

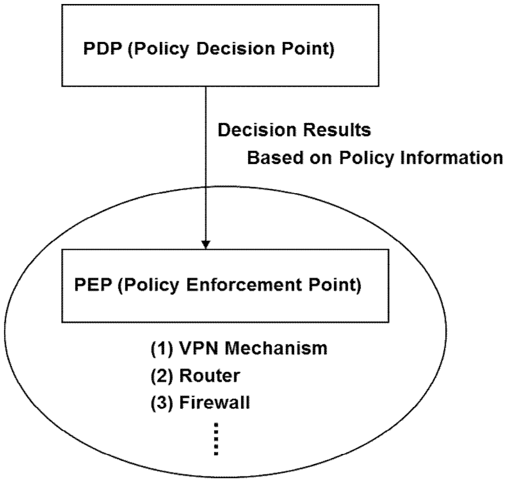

PDP (Policy Decision Point)
Decision Results
Based on Policy Information
PEP (Policy Enforcement Point)
(1) VPN Mechanism
(2) Router
(3) Firewall

Figure 2. Essential Principle

However, all the frameworks explained above are based on the principle shown in Figure 1. As problems of these frameworks, two points are presented as follows. Essential principle is described in Figure 2. Concretely, in the point called Policy Decision Point (PDP) judgment, such as permission and non-permission for communication pass is performed based on policy information. The judgment is notified and transmitted to the point called the PEP, which is the mechanism, such as VPN mechanism, router and Fire wall, which is located on the network path among hosts (servers and clients). Based on that judgment, the control is added for the communication that is going to pass by.

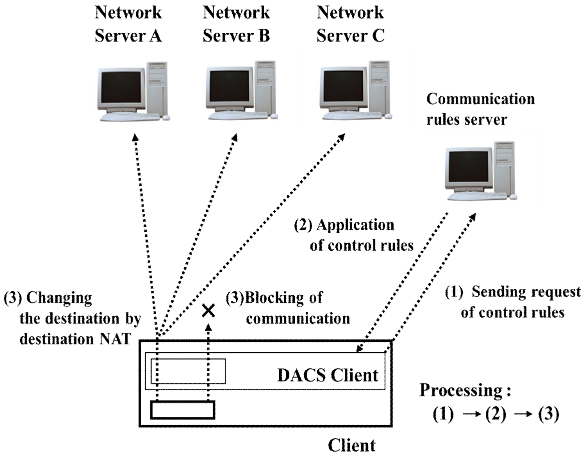

Network Server A
Network Server B
Network Server C
Communication rules server
(2) Application of control rules
(3) Changing the destination by destination NAT
(3)Blocking of communication
(1) Sending request of control rules
DACS Client
Processing : (1) → (2) → (3)
Client

Figure 3. Principle in Scheme to Control on a Client

The principle of the scheme for controlling on a client is described in Figure 3.By locating the communication control mechanisms on the clients, the whole LAN is managed. Because this scheme controls the network communications on each client, the processing load is low. However, because the communication control mechanisms need to be located on each client, the work load becomes heavy.

When it is thought that Internet system is managed by using these two schemes, it is difficult to put a control unit on the network course practically. The communication control mechanism needs to be located on the path between network servers and clients without exception. This is why, we devised the scheme for controlling the network on a client. The scheme locates the communication controls mechanisms on each client. That is, the software for communication control is installed on each client. So, by devising the installing mechanism letting users install software to the client easily, it becomes possible to apply the scheme for controlling the network on a client to Internet system. As a first step for the last goal, we showed the Wide Area DACS system (wDACS) system [15]. This system manages a wide area network, which one organization manages. Therefore, it is impossible for plural organizations to use this system. Then, as the first step of the second phase, we showed the concept of the cloud type virtual PBNM, which could be used by plural organizations in this paper.

III. EXISTING DACS SCHEME AND WDACS SYSTEM

In this section, the content of the DACS Scheme, which is the study of the phase 1 is described.

A Basic Principle of the DACS Scheme

Figure 4 shows the basic principle of the network services by the DACS Scheme. At the timing of the (a) or (b) as shown in the following, the DACS rules (rules defined by the user unit) are distributed from the DACS Server to the DACS Client.

(a) At the time of a user logging in the client.

(b) At the time of a delivery indication from the system administrator.

According to the distributed DACS rules, the DACS Client performs (1) or (2) operation as shown in the following. Then, communication control of the client is performed for every login user.

(1) Destination information on IP Packet, which is sent from application program, is changed.

(2) IP Packet from the client, which is sent from the application program to the outside of the client, is blocked.

An example of the case (1) is shown in Figure 4. In Figure 4, the system administrator can distribute a communication of the login user to the specified server among servers A, B or C. Moreover, the case (2) is described. For example, when the system administrator wants to forbid an user to use MUA (Mail User Agent), it will be performed by blocking IP Packet with the specific destination information.

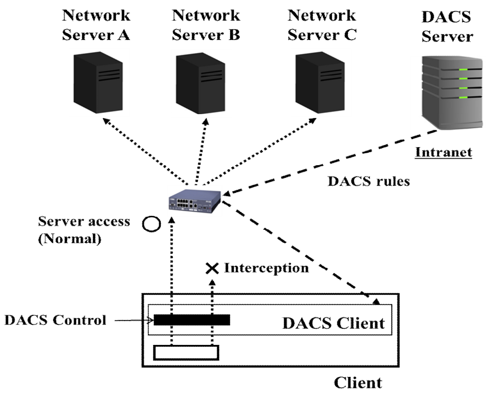


Figure 4. Basic Principle of the DACS Scheme

In order to realize the DACS Scheme, the operation is done by a DACS Protocol as shown in Figure 5. As shown by (1) of the double way arrow between DACS Server and IN block in Figure 5, the distribution of the DACS rules is performed on communication between the DACS Server and the DACS Client, which is arranged at the application layer. The application of the DACS rules to the DACS Control is shown by (2) in Figure 5.

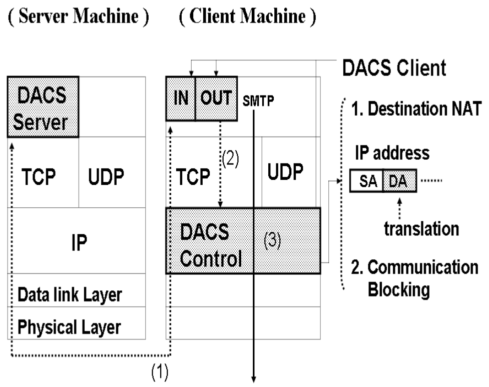


Figure 5. Layer Setting of the DACS Scheme

The steady communication control, such as a modification of the destination information or the communication blocking is performed at the network layer as shown by (3) in Figure 5.

B Communication Control on Client

The communication control on every user was given. However, it may be better to perform communication control on every client instead of every user. For example, it is the case where many and unspecified users use a computer room, which is controlled. In this section, the method of communication control on every client is described, and the coexistence method with the communication control on every user is considered.

When a user logs in to a client, the IP address of the client is transmitted to the DACS Server from the DACS Client. Then, if the DACS rules corresponding to IP address, is registered into the DACS Server side, it is transmitted to the DACS Client. Then, communication control for every client can be realized by applying to the DACS Control. In this case, it is a premise that a client uses a fixed IP address. However, when using DHCP service, it is possible to carry out the same control to all the clients linked to the whole network or its subnetwork for example.

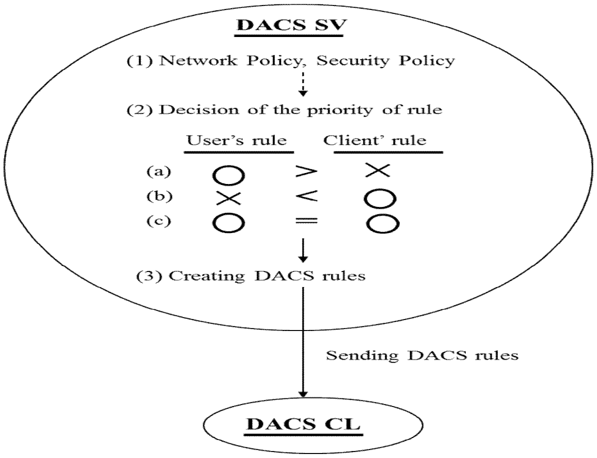


Figure 6. Creating the DACS rules on the DACS Server

When using communication control on every user and every client, communication control may conflict. In that case, a priority needs to be given. The judgment is performed in the DACS Server side as shown in Figure 6. Although not necessarily stipulated, the network policy or security policy exists in the organization such as a university (1). The priority is decided according to the policy (2). In (a), priority is given for the user's rule to control communication by the user unit. In (b), priority is given for the client's rule to control communication by the client unit. In (c), the user's rule is the same as the client's rule. As the result of comparing the conflict rules, one rule is determined respectively. Those rules and other rules not overlapping are gathered, and the DACS rules are created (3). The DACS rules are transmitted to the DACS Client. In the DACS Client side, the DACS rules are applied to the DACS Control. The difference between the user's rule and the client's rule is not distinguished.

C Security Mechanism of the DACS Scheme

In this section, the security function of the DACS Scheme is described. The communication is tunneled and encrypted by use of SSH. By using the function of port forwarding of SSH, it is realized to tunnel and encrypt the communication between the network server and the DACS Client, which is installed in the client. Normally, to communicate from a client application to a network server by using the function of port forwarding of SSH, local host (127.0.0.1) needs to be indicated on that client application as a communicating server. The transparent use of a client, which is a characteristic of the DACS Scheme, is failed. The transparent use of a client means that a client can be used continuously without changing setups when the network system is updated. The function that doesn't fail the transparent use of a client is needed. The mechanism of that function is shown in Figure 7.

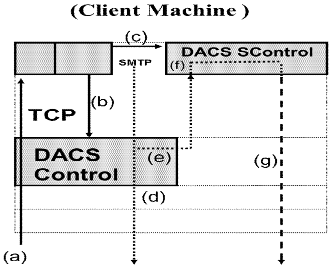


Figure 7. Extend Security Function

D Application to cloud environment

In this section, the contents of wDACS system are explained in Figure 8. First, as preconditions, because private IP addresses are assigned to all servers and clients existing in from LAN1 to LAN n, mechanisms of NAT/NAPT are necessary for the communication from each LAN to the outside. In this case, NAT/NAPT is located on the entrance of the LAN such as (1), and the private IP address is converted to the global IP address towards the direction of the arrow. Next, because the private IP addresses are set on the servers and clients in the LAN, other communications except those converted by Destination NAT cannot enter into the LAN. But, responses for the communications sent form the inside of the LAN can enter into the inside of the LAN because of the reverse conversion process by the NAT/NAPT. In addition, communications from the outside of the LAN1 to the inside are performed through the conversion of the destination IP address by Destination NAT. Concretely, the global IP address at the same of the outside interface of the router is changed to the private IP address of each server. From here, system configuration of each LAN is described. First, the DACS Server and the authentication server are located on the DMZ on the LAN1 such as (4). On the entrance of the LAN1, NAT/NAPT and destination NAT exists such as (1) and (2). Because only the DACS Server and network servers are set as the target destination, the authentication server cannot be accessed from the outside of the LAN1. In the LANs form LAN 2 to LAN n, clients managed by the wDACS system exist, and NAT/NAPT is located on the entrance of each LAN such as (1). Then, F/W such as (3) or (5) exists behind or with NAT/NAPT in all LANs.

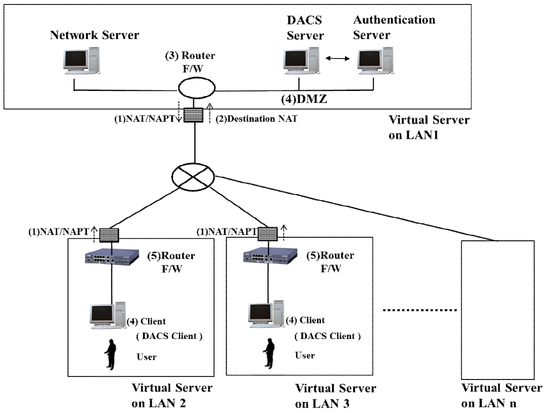


Figure 8. Basic System Configuration of wDACS System

IV. THE CLOUD TYPE VIRTUAL PBNM FOR THE COMMON USE BETWEEN PLURAL ORGANIZATIONS

In this section, after the concept and implementation of the proposed scheme were described, functional evaluation results are described.

A. Concept of the Cloud Type Virtual PBNM for the Common Use Between Plural Organizations

In Figure 9, which is described in [16], the proposed concept is shown. Because the existing wDACS Scheme realized the PBNM control with the software called the DACS Server and the DACS client, other mechanism was not needed. By this point, application to the cloud environment was easy.

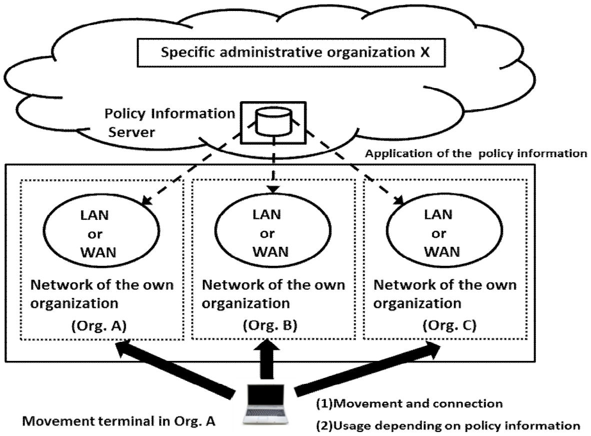

Specific administrative organization X
Policy Information
Server
Application of the policy information
LAN
or
WAN
Network of the own organization
(Org. A)
LAN
or
WAN
Network of the own organization
(Org. B)
LAN
or
WAN
Network of the own organization
(Org. C)
Movement terminal in Org. A
(1)Movement and connection
(2)Usage depending on policy information

Figure 9. Concept of the Proposed Scheme

B. Implementation of the basic function in the

The proposed scheme in this paper realizes the common usage by plural organizations by adding the following elements to realize the common usage by plural organizations: user identification of the plural organizations, management of the policy information of the plural organizations, application of the PKI for code communication in the Internet, Redundant configuration of the DACS Server (policy information server), load balancing configuration of the DACS Server, installation function of DACS Client by way of the Internet .

C. Cloud Type Virtual PBNM for the Common Usage Between Plural Organizations

In the past study [14], the DACS Client was operated on the windows operation system (Windows OS). It was because there were many cases that the Windows OS was used for as the OS of the client. However, the Linux operating system (Linux OS) had enough functions to be used as the client recently, too. In addition, it was thought that the case used in the clients in the future came out recently. Therefore, to prove the possibility of the DACS Scheme on the Linux OS, the basic function of the DACS Client was implemented in this study. The basic functions of the DACS Server and DACS Client were implemented by JAVA language. From here, it is described about the order of the process in the DACS Client and DACS Server as follows.

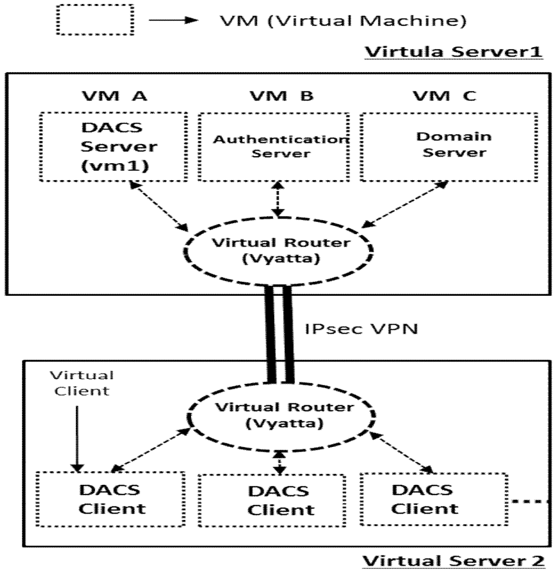


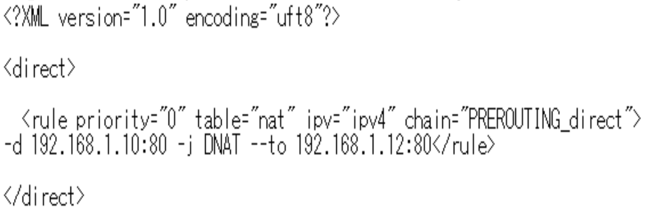
Figure.10 Prototype System

(Processes in the DACS Client)
(p1) The information acquisition from Cent OS
(p2) Transmission from the DACS Client to the DACS
(p3) The information transmission from the DACS Client to
(p4) The reception of the DACS rules from the DACS Server
(p5) Application of the DACS rules of the DACS Control

(Processes in the DACS Server)
(p1) The information reception from the DACS Client
(p2) Connection to the database
(p3) Inquiry of the Database
(p4) Transmission of the DACS rules to the DACS Client

D. Results of the functional evaluation

In this section, the results of the functional evaluation for the implementation system are described in Figure 10.



```
<?XML version="1.0" encoding="uft8"?>

<direct>

  <rule priority="0" table="nat" ipv="ipv4" chain="PREROUTING_direct">
-d 192.168.1.10:80 -j DNAT --to 192.168.1.12:80</rule>

</direct>
```

Figure.11 Setting Situation of the DACS rules on the DACS CL

In Figure 11, the setting situation of the DACS rules is described in figure 11. This DACS rules is the rule to change a Web server for the access. The delivery of the DACS rules is between the DACS SV and the DACS CL encrypted by using SSL.

By this DACS rules, the next operation was realized. When the user accessed the Web Server with the IP address of 192.168.1.10, the Web Server with the IP address of 192.168.1.12 was accessed actually. As for this communication result, the communication log on each Web server was confirmed by viewing.

V. Load Experiment Results

In this section, after the description of experimental environment, load experiment results are described.

A. Load experiment results to confirm the function of the software for realization of the Cloud Type Virtual PBNM for the Common Use Between Plural Organizations

In this section, the load experiment results are described. In the Figure 12, the experimental environment is described. This environment consists of four virtual servers. In the virtual server 1, servers group such as the DACS Server and user authentication server is stored. In other virtual severs such as the virtual server 2, virtual server 3 and virtual server 4, the virtual client, which is installed the DACS Client is stored. The number of the virtual clients is 100.

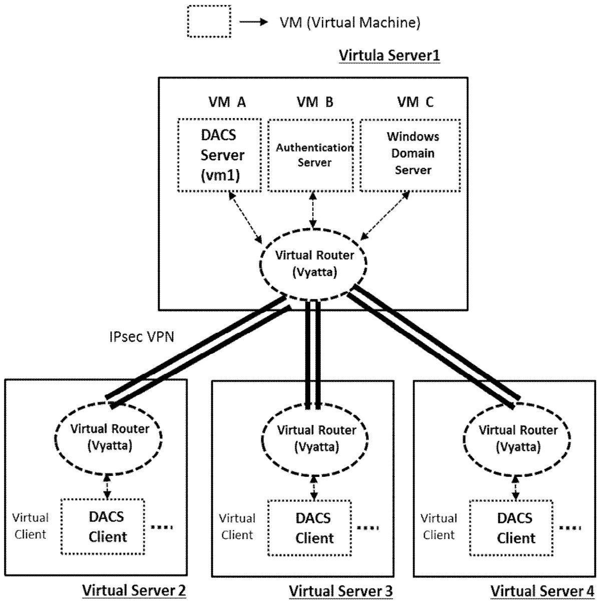
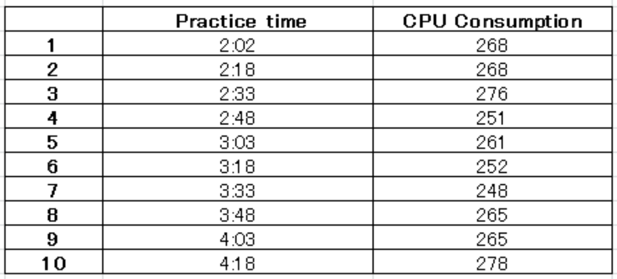


Figure.12 Experimental Environment

By using this experimental environment, the load experiment was executed. Specifically, simultaneous accesses for the DACS SV from the 100 virtual clients were performed at the rate of one time form 15 minutes. The number of the simultaneous connections for the DACS SV was set to 10 on this occasion. The experimental results are described in Table 1.

TABLE I. EXPERIMENTAL RESULTS (1)



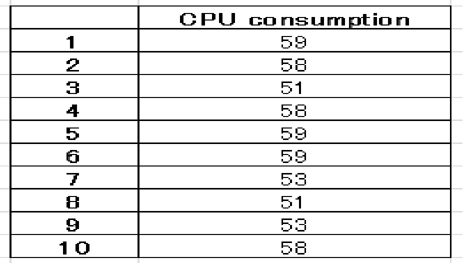
	Practice time	CPU Consumption
1	2:02	268
2	2:18	268
3	2:33	276
4	2:48	251
5	3:03	261
6	3:18	252
7	3:33	248
8	3:48	265
9	4:03	265
10	4:18	278

In this table, the practice time of the DACL CL and CPU consumption is described. The average of the results of the

Copyright (c) IARIA, 2017. ISBN: 978-1-61208-554-8

measurement for ten times was 263.2 MHz. This value is around three times of the value shown in Table 2.

TABLE II. EXPERIMENTAL RESULTS (2)



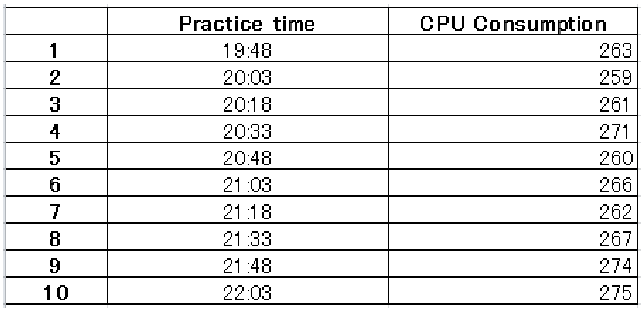
	CPU consumption
1	59
2	58
3	51
4	58
5	59
6	59
7	53
8	51
9	53
10	58

In the experiment of the Table 2, the Windows client is used, and the communications between the DACS SV and the DACS CL is not encrypted. In this experiment, the Linux client is used, and the communications between the DACS SV and the DACS CL is encrypted by SSL. Particularly, because an element of the overhead processes of the SSL is large, it is thought that such a result was derived.

B. Load experiment results for applications to the small and medium size scale organization

In this section, the load experiment results are described. The experimental environment is described. The experimental environment is as previous experiment environment. In this experiment, simultaneous accesses for the DACS SV from the 200 virtual clients were performed at the rate of one time form 15 minutes. The number of the simultaneous connections for the DACS SV was set to 10 on this occasion. The experimental results are described in Table 3.

TABLE III. EXPERIMENTAL RESULTS (3)



	Practice time	CPU Consumption
1	19:48	263
2	20:03	259
3	20:18	261
4	20:33	271
5	20:48	260
6	21:03	266
7	21:18	262
8	21:33	267
9	21:48	274
10	22:03	275

In this table, the average of the results of the measurement for ten times was 265.8 MHz. This value is same as the value shown in Table 1. In other words, when the number of the client is 200, CPU consumption of the DACS SV becomes the constant standard by limiting the number of simultaneous connections to 10.

VI. CONCLUSION

In this paper, we performed the load experiment of the cloud type virtual PBNM, which can be used by plural organizations. In this experiment, the 200 virtual clients with Linux OS are used, and the communications between the DACS SV and the DACS CL are encrypted. The number of the simultaneous connections for the DACS SV was set to 10 on this occasion. As the result, the average of CPU consumption was 265.8 MHz. It became possible to confirm the fact that CPU consumption of the DACS SV becomes about 263~265MHz by limiting the number of simultaneous connections to 10. By this experiment, it was confirmed this proposed scheme was applicable to the network with the 200 clients.

As a future work, we are going to perform more load experiments in the form of changing the number of the virtual clients and the number of the simultaneous connections for the DACS SV to show that it is applicable in a small and medium size scale network with the clients of around 1000.

ACKNOWLEDGMENT

This work was supported by the research grant of KDDI Foundation. We express our gratitude.

REFERENCES

[1] V. Cerf and E. Kahin, “A Protocol for Packet Network Interconnection,” IEEE Trans. on Commn, vol.COM-22, May 1974, pp.637-648.

[2] R. Yavatkar, D. Pendarakis, and R. Guerin, “A Framework for Policy-based Admission Control, ” IETF RFC 2753, 2000.

[3] B. Moore, E. Ellesson, J. Strassner, and A. Westerinen, “Policy Core Information Model -- Version 1 Specification, ” IETF RFC 3060, 2001.

[4] B. Moore., “Policy Core Information Model (PCIM) Extensions, ” IETF 3460, 2003.

[5] J. Strassner, B. Moore, R. Moats, and E. Ellesson, “ Policy Core Lightweight Directory Access Protocol (LDAP) Schema,” IETF RFC 3703, 2004.

[6] D. Durham at el., “The COPS (Common Open Policy Service) Protocol, ” IETF RFC 2748, 2000.

[7] S. Herzog at el., “COPS usage for RSVP,” IETF RFC 2749, 2000.

[8] K. Chan et al., “COPS Usage for Policy Provisioning (COPS-PR),” IETF RFC 3084, 2001.

[9] CIM Core Model V2.5 LDAP Mapping Specification, 2002.

[10] M. Wahl, T. Howes, and S.Kille, “Lightweight Directory Access Protocol (v3),” IETF RFC 2251, 1997.

[11] CIM Schema: Version 2.30.0, 2011.

[12] ETSI ES 282 003: Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN); Resource and Admission Control Subsystem (RACS); Functional Architecture, June 2006.

[13] ETSI ETSI ES 283 026: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification, April 2006.

[14] K. Odagiri, R. Yaegashi,M. Tadauchi, and N. Ishii, “Secure DACS Scheme, “Journal of Network and Computer Applications,” Elsevier, Vol.31, Issue 4, 2008, pp.851-861, November.