INNOV 2016

The Fifth International Conference on Communications, Computation, Networks and Technologies

ISBN: 978-1-61208-503-6

August 21 - 25, 2016

Rome, Italy

INNOV 2016 Editors

Jaime Lloret Mauri, Polytechnic University of Valencia, Spain

Pascal Lorenz, University of Haute Alsace, France

INNOV 2016

Forward

The Fifth International Conference on Communications, Computation, Networks and Technologies (VALID 2016), held on August 21 - 25, 2016 in Rome, Italy, aimed at addressing recent research results and forecasting challenges on selected topics related to communications, computation, networks and technologies.

Considering the importance of innovative topics in today's technology-driven society, there is a paradigm shift in classical-by-now approaches, such as networking, communications, resource sharing, collaboration and telecommunications. Recent achievements demand rethinking available technologies and considering the emerging ones.

The conference had the following tracks:

□ Networking
□Mobility and Ubiquity
□Security, Trust, and Privacy

We take here the opportunity to warmly thank all the members of the INNOV 2016 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 that dedicated much of their time and effort to contribute to INNOV 2016. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations and sponsors. We also gratefully thank the members of the INNOV 2016 organizing committee for their help in handling the logistics and for their work that made this professional meeting a success.

We hope that INNOV 2016 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in the areas of communication, computation, networks and technologies. We also hope Rome provided a pleasant environment during the conference and everyone saved some time for exploring this beautiful historic city.

INNOV 2016 Advisory Committee

Seah Boon Keong, MIMOS Berhad, Malaysia
Mike Johnstone, Edith Cowan University, Australia
Carlos Becker Westphall, University of Santa Catarina, Brazil
Jaime Lloret Mauri, Polytechnic University of Valencia, Spain

INNOV 2016

Committee

INNOV 2016 Advisory Committee

Seah Boon Keong, MIMOS Berhad, Malaysia
Mike Johnstone, Edith Cowan University, Australia
Carlos Becker Westphall, University of Santa Catarina, Brazil
Jaime Lloret Mauri, Polytechnic University of Valencia, Spain

INNOV 2016 Technical Program Committee

Omar Alhazmi, Taibah University, Saudi Arabia
Alargam Elrayah Elsayed Ali, University of Khartoum, Sudan
Wan D. Bae, University of Wisconsin-Stout, USA
Henri Basson, University of Lille North of France, France
Michael Bauer, The University of Western Ontario, Canada
Carlos Becker Westphall, University of Santa Catarina, Brazil
Khalid Benali, LORIA - Université de Lorraine, France
Eugen Borcoci, University Politehnica of Bucharest, Romania
Albert M. K. Cheng, University of Houston, USA
Grzegorz Chmaj, University of Nevada - Las Vegas, USA
Li-Der Chou, National Central University, Taiwan
Morshed U. Chowdhury, Deakin University-Melbourne Campus, Australia
Jacques Demongeot, IMAG/University of Grenoble, France
Uma Maheswari Devi, IBM Research, India
Dimitris Dranidis, International Faculty of the University of Sheffield, CITY College, Greece
Mohamed Y. Eltabakh, Computer Science Department - Worcester Polytechnic Institute, USA
Agata Filipowska, Poznan University of Economics, Poland
David A. Gustafson, Kansas State University, USA
Fred Harris, University of Nevada - Reno, USA
Houcine Hassan, Universitat Politecnica de Valencia, Spain
Qiang He, School of Software and Electrical Engineering - Swinburne University of Technology, Australia
Pao-Ann Hsiung, National Chung Cheng University, Taiwan
Yu-Chen Hu, Providence University, Taiwan
Kuo-Chan Huang, National Taichung University of Education, Taiwan
Shih-Chang Huang, National Formosa University, Taiwan
Yo-Ping Huang, National Taipei University of Technology, Taiwan
Sajid Hussain, Fisk University, Nashville, USA
Tazar Hussain, King Saud University (KSU) - Riyadh, Kingdom of Saudi Arabia
Wen-Jyi Hwang, National Taiwan Normal University, Taiwan
Sergio Ilarri, University of Zaragoza, Spain
Abdessamad Imine, LORIA-INRIA, France
Wassim Jaziri, Taibah University, Saudi Arabia

Copyright Information

Table of Contents

Using Sensor Technology to Monitor and Report Vandalized Pipelines

Mohammed Yusuf Agetegba
College of Computer Science and Information Technology
Sudan University of Science and Technology
Khartoum, Sudan
email: mylislan@yahoo.com

Prof. Pascal Lorenz
University of Haute Alsace
34 rue du Grillenbreit, Colmar - France.
email: pascal.lorenz@uha.fr

Abstract— **Pipelines transporting gasoline, diesel, crude, and natural gas are periodically subjected to acts of vandalism and sabotage in Nigeria. Unfortunately, vandalized pipelines are not quickly detected; leading to major environmental degradation, and in case of gasoline, to explosion and attendant loss of lives and properties. Since it is nearly impossible for security operatives to monitor large sections of Nigerian national pipelines, it becomes imperative to propose smart solutions which allow monitoring of pipelines using wireless sensors. This paper proposes the use of wireless sensors to monitor acoustics, vibrations and lights emanating from or around targeted pipelines. Sound detection process automatically triggers verification, which involves turning on the sensor to detect pipeline vibration. A night-time mode allows the sensor to equally scan for bright lights which may connote a pipeline on fire. The paper strives to lay a solid foundation for full deployment of actual motes. We propose the use of linear clustering to ensure energy conservation.**

Keywords—Pipelines; Motes; Wireless; Sound; Acoustic.

I. INTRODUCTION

Various environmental monitoring projects using wireless sensors successfully demonstrated the ability of sensors to monitor changes in their deployed environment (such as ambience, movement, and stress in concrete) and report findings [6][7][12]. While designing wireless sensors monitoring systems, it is imperative to painstakingly gather environmental data which forms the parameters on which the algorithm controlling each mote will operate. Parameters gathered for our pipeline monitoring project include: (1) pipeline - material (iron, steel etc.), (2) thickness, (3) diameter, (4) normal vibration while conveying crude, gasoline, diesel or liquefied gas, and (5) topography and settlement type through which the pipeline passes (swamp, rivers, forests, underground, villages, towns etc.). Each parameter directly affects the distance, vibration and acoustic velocity, which are important parameters in our proposed project.

Wireless Sensor Networks (WSNs) are made up of a great number of sensors. These sensors are called sensor nodes, whose main purpose more often than not are to sense, process, and transmit information about the deployed environment or surrounding [5][6][7]. These sensors are usually dispersed in an environment or different location for the purpose of information gathering [3][6]. The acquired information is transmitted to a central sink node so that users could have access remotely through a gateway. A sensor node comprises of either one or more sensors, a signal conditioning unit, an analog to digital conversion module (ADC), a central processing unit (CPU), Memory, a radio transceiver and an energy power supply unit as depicted in Fig. 2 [5][12]. Subject to application or deployment environment, sensors are often protected to guard against physical, chemical, etc. damage.

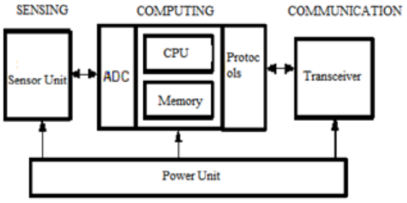


Figure 1. Wireless Sensor Node Architecture

Sensors nodes can be obtained off-the-shelf in two forms: 1. Generic (general-purpose) nodes and 2. Gateway (bridge) nodes [4]. A generic (general-purpose): the function of this kind of sensor node is to obtain measurements from the environment being monitored [5]. It is often equipped with different mechanisms which are capable of measuring various elements or environmental traits such as light, temperature, humidity, barometric pressure, velocity, acceleration, acoustics, magnetic field, etc. Gateway (bridge): the function of this type of node is to collect information from generic sensors and transmit to the base station. Gateway nodes are equipped with greater processing capability, stronger battery power, and a longer transmission (radio) range [3]. A mixture of generic and gateway nodes are usually set up to create a WSN [3][4].

Our proposed wireless sensor motes can function in two ways:

- As full function device (FFD): The FFD is a midway router whose function is to relay data collected from other devices. It does not require large memory which makes it less expensive to develop. It can function in all WSN topologies and can operate as a coordinator.
- As reduced function device (RFD): This device only transmit its host’s or environment’ physical attributes that is, it just transmits to the network coordinator only; it does not convey data from other devices. It in fact requires less memory than FFD (very little RAM and ROM, no flash); this makes it even cheaper to develop than an FFD. RFD is easier to implement on star topology.

This paper proposes the use of wireless sensors to monitor pipelines by observing parameters such as pipeline acoustics, vibrations and ambience lights around pipelines. Our proposed project conserves energy by eliminating recording of detected acoustics and predictively control mote's wake up and radio usage functionalities. To further conserve energy, we adopted network segmentation through linear clustering [8][10][11][13]. Linear clustering was adopted based on research work by Alnuem [13], who demonstrated higher energy consumption when nodes are widely spaced.

Figure 2 below illustrates the diverse terrain (swamp, villages, towns, forests, roadside etc) through which Nigerian pipelines are deployed.

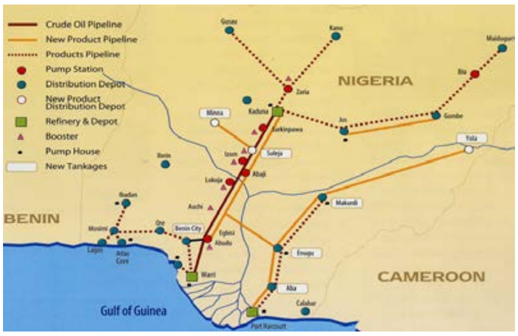


Figure 2. Nigerian Pipelines Network

The remainder of this paper is organized as follows: Section II discusses the state of the art which explores various methods used to monitor pipelines for vandalism, natural disaster, and leakages, while the proposed work, which comprises the system architecture, the mote configuration, the mote deployment, the mote security and the mote/Gateway messaging are discussed and illustrated in Section III. Section IV presents and discusses the simulation results. Finally, Section V concludes the paper and points out open research issues and further research works.

II. STATE OF THE ART

Several methods have been devised in order to monitor and report pipeline status. The most common and popular ones includes Acoustic Sensors – this employs acoustic or vibration measurement for pipeline monitoring [2][17][18]. Vision based systems – this is based on PIG (Pipeline Inspection Gauge) which must be inserted into the pipe. It works like image processor or laser scanner which main function is to detect leakages [2][18]. Ground penetrating radar (GPR) based systems – this is best suitable for use on environment with dry soil, but is not good for large network of pipes monitoring [2][17][18]. Fiber optic Sensors - this is suitable for present day pipeline monitoring systems, it can handle most present day pipelines issues, some of its drawbacks is the probability for redundancy and some challenges with deployment [2][13]. Multi modal underground wireless system – this uses low power, as the name implies it is meant for an underground installation, it has the advantage of camouflaging, but one of the disadvantages is that it has to be buried underground, that is a trench has to be created [2][18]. Every single Sensor has a distinctive feature and typical operating condition. Choosing a sensor for pipeline monitoring to a large extent depends on the environment to be deployed and the deployment method.

This research work recommends wireless motes from both *MICA series and IRIS* (to monitor pipelines and report either ongoing attempts to vandalize sections of a pipeline or to quickly report ruptured pipelines.

Ismail et al. [1] demonstrated the ability of IRIS and MICAz mote to detect and record sounds while eliminating ambient noise levels. Their paper allow a parent mote to assign recording tasks to motes within their cluster.

Lou et al. [17] demonstrated the ability of MICAz to detect and record environmental acoustics using the Microphone on MTS310CA sensor boards.

Kim et al. [18] also show the feasibility of using MICA based mobile wireless sensor with attached RFID in pipe line monitoring and maintenance.

This paper differs from [1][17][18] in the following areas : (1) Detected sound is not recorded. (2) Only very loud sounds triggers verification of sound source. Verification of detected sound is necessary due to the likelihood that certain persistent ambient sounds can trigger sound detection, hence the project introduces additional layers of checks, such as checking for pipeline vibration, detecting temperature and measuring magnetic flow around the pipeline. Finally, a night-time mode of operation allows base station to activate light sensors on deployed FFD motes. This enable FFD motes to detect and report fire around the pipeline. (4) Motes are deployed using “Linear Clustering”. Figure 3 below represents our proposed test environment.

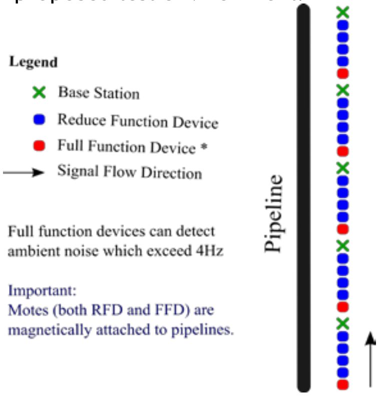

Legend
✕ Base Station
● Reduce Function Device
● Full Function Device *
Signal Flow Direction
Full function devices can detect ambient noise which exceed 4Hz
Important:
Motes (both RFD and FFD) are magnetically attached to pipelines.
Pipeline

Figure 3. Proposed mote deployment (motes are magnetically attached to pipeline)

III PROPOSED WORK

This paper recommends using wireless motes to (1) sense ambient sounds, (2) confirm the type of sound by testing pipeline vibration and magnetic flow around monitored pipeline, (3) if operating under night-time mode; check for fire using both temperature and light sensors, (4) finally, the mote sends it's ID to designated base station or sink. MICAz and IRIS are compatible and can use similar sensor boards, since both are equipped with similar 51 pins sensor connector module. However, MEMSIC IRIS has better radio range and a larger memory capacity when compared with previous MICA motes [14].

Figures 4, 5 and 6 below depict deferent kinds of motes for the proposed project.

Figure.4. MICA2

Figure 5. MICAz

Figure 6. IRIS

Each mote has a 51 pin connector interface which allow MTS310CA sensor boards to connect to the mote. The sensing capabilities [14] of MTS310CA sensor board are (1) light detection (2) temperature detection (3) sound detection (4) acceleration and vibration sensing and (5) magnetic field detection [14].

A. *Proposed Mote Configuration*

Two kinds of motes will be deployed to achieve proposed objectives, namely motes equipped with MTS310CA sensor boards (also known as full function devices or FFD), and those without the sensor board (known as Reduced Function Devices or RFD).

B. *Sound Sensing*

Sound sensing triggers other sound verification events in quick succession. This process avoids false alarm and stabilizes system credibility. Hence sound sensing motes must be properly configured to detect sounds above topographical ambience levels. However, setting a high frequency level can force the device not to detect certain frequencies, for example, a large explosion has a frequency of between 20Hz to 50Hz, however, when explosions rips through metal, the frequency increases and can be detected by a sound sensing mote. Another interesting fact about sound is the fixed distance within which generated wavelength can propagate; depending on the velocity. Sound velocity is determined either by environment (temperature) or the composition of the material through which the sound propagates (such as air, water, iron and steel). For example, Given the following values, let us calculate the distance covered by a large explosion through an empty steel pipe:

$$Given: \ Sound\ velocity\ through\ empty\ steel\ pipe\ (v) = 5960$$
$$Given: Explosion\ frequency\ (f) = 50\,Hz$$

$$formula: \ \lambda = \frac{v}{f}$$

$$therefore: \ \lambda = \frac{5960}{50}$$

$$= 199\,meters \ \text{ or } \ 391.08\,feets$$

A knowledge of the distance covered by each sound wavelength influences placement of sound sensing motes. The Table.1 lists the various ambient sounds common along the route of Nigerian pipelines:

TABLE 1. AMBIENT SOUNDS COMMON ALONG THE ROUTE OF NIGERIAN PIPELINES

Source	**Decibel**	**Frequency (Hz)**
Chain Saw	100 db	2000 Hz
Chirping Bird	5 db	7000 Hz
Rustling Leaves	>2 db	1500 Hz
Gunshot	>120 db	2000 Hz
Festive Band	110 db	800-1500 Hz
Crying, talking, barking dog	30 – 60 db	250 – 700 Hz

C. *Proposed Motes Deployment*

The proposed Motes are deployed in such a way that Full Function Devices are positioned to prevent simultaneous sensing of same sound (due to sound propagation) Figure 3 above. However, in the rare event that it does happen, operators will be able to locate the actual sound source by examining transmitted ID of motes that reported the sound within a linear cluster.

"Linear Clustering" allow a group of Full and Reduced function devices to be either "linearly attached" to surface pipelines or to trees, rocks and other naturally occurring feature over an underground pipeline. Each group/cluster of FFDs and RFDs relay monitoring results to a base station as shown in Figures 7 and 8 below.

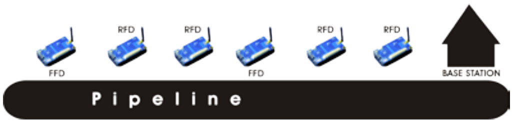


Figure 7. Cluster of FF and RF Devices on a surface pipeline. Cluster will be repeated along total distance of surface pipeline

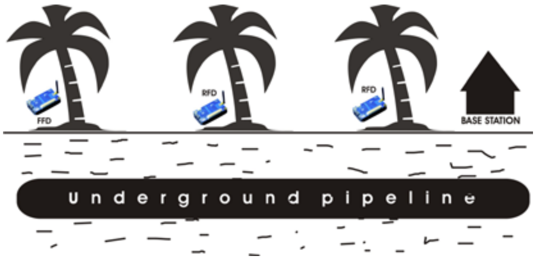


Figure 8. Cluster of FF and RF Devices placed on trees along the path of underground pipeline. Cluster will be repeated along total distance of underground pipeline

Distances between Full Function and Reduced Function Devices will be determined by both lowest acoustic worth detecting and the maximum range of wireless broadcast.

Monitoring underground pipeline against vandalism is achieved through constant monitoring of ambience acoustics along underground pipeline deployment route.

Emphasis is laid on monitoring attempts to excavate sections of top soil above underground pipelines. Motes saddled with monitoring these sections will be programmed to detect voices, excavating machinery, chainsaws etc.

As stated earlier, both surface and underground pipelines adopt linear clustering to both enhance communication and minimize power consumption.

However, a stolen or malfunction mote within a cluster will greatly affect transmission of verified attempts on a pipeline.

D. *Mote Security*

Motes will be required to periodically send identifying information every 72 hours to the base station. Failure to receive such information enable operators to know what motes to replace (either lost to theft, drained batteries, or simply damaged).

E. *Mote/Gateway Messaging*

Mote's ability to properly monitor pipelines can be jeopardized if sound sensing motes are not aware of changes in pipeline status. For example, is it empty or is it crude, gasoline or diesel flowing through it? Therefore, operators need to inform motes wirelessly when crude is being pumped along pipelines. This enable sound sensing motes to adjust their sound sensing algorithm. We equally propose a night-time mode for FFD sensors, this mode is trigger via a message received from the base station. It allows sensors to include temperature and light sensing during each pipeline monitoring cycle.

Base station operators remotely notify motes regarding both pipeline status and day time/night time status. Pipeline status notifies motes when liquid is being pumped through pipelines or when pipeline are empty. Such notifications enable motes to know what sensors to engage during each sampling process.

Similarly, night time/day time status notification determines the various sensors a mote will utilize during each predetermined round of ambience sampling.

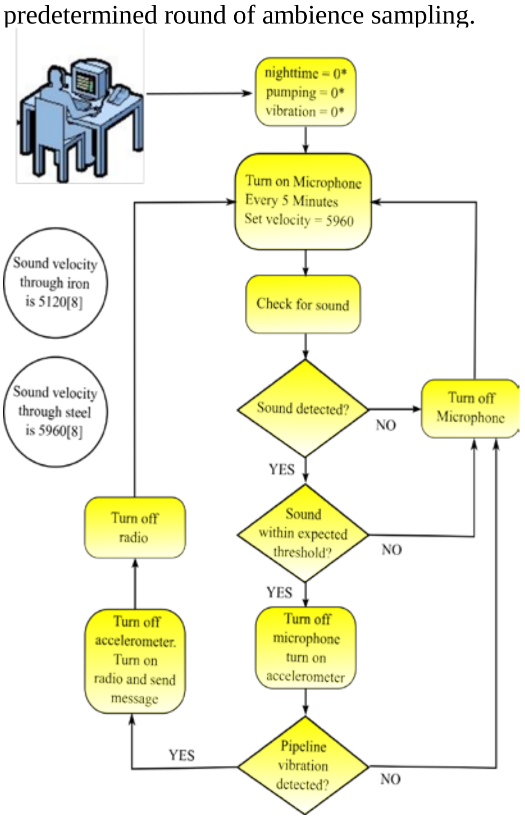

nighttime = 0*
pumping = 0*
vibration = 0*
Turn on Microphone
Every 5 Minutes
Set velocity = 5960
Sound velocity through iron is 5120[8]
Sound velocity through steel is 5960[8]
Check for sound
Sound detected?
NO
Turn off Microphone
YES
Sound within expected threshold?
NO
YES
Turn off radio
Turn off accelerometer. Turn on radio and send message
Turn off microphone turn on accelerometer
YES
Pipeline vibration detected?
NO

Figure 9. Flow chart represents action to be taken during the day when nothing is being pumped through the pipeline. In TinyOS 0 or false is 1

The process flowchart (above, Fig.9) represents actions to be taken by FFD motes during the day, when pipelines are empty (that is when nothing is being pumped through pipelines). The process flowchart eliminates false “alerts” caused by high frequency sounds such as the chirping of a bird by checking if detected sound lead to pipeline vibration.

A detected pipeline vibration triggers the next action which involves turning on the radio and transmitting sensor's ID to the base station. Transmitted ID is used by base station operators to identify sensor's coordinate along the pipeline.

The next process flowchart (Fig. 10) represents algorithm to execute during the day, when pipeline is in use (that is when crude or related products are being pumped through pipelines).

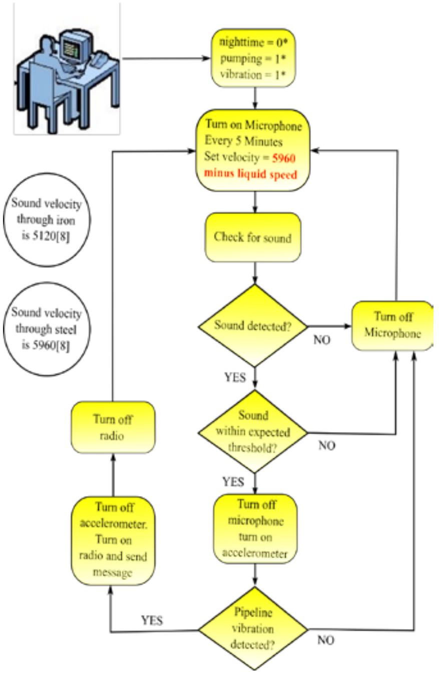

nighttime = 0*
pumping = 1*
vibration = 1*
Turn on Microphone
Every 5 Minutes
Set velocity = 5960
minus liquid speed
Sound velocity through iron is 5120[8]
Sound velocity through steel is 5960[8]
Check for sound
Sound detected?
NO
Turn off Microphone
YES
Sound within expected threshold?
NO
YES
Turn off radio
Turn off accelerometer. Turn on radio and send message
Turn off microphone turn on accelerometer
YES
Pipeline vibration detected?
NO

Figure 10. The flow of crude oil or related product triggers slight vibration

Finally, the next two process flow chart uses light and temperature sensors (in addition to acoustic and accelerometer, (Figures 11 and 12) during **nighttime** mode to detect acts of vandalism against the pipe.

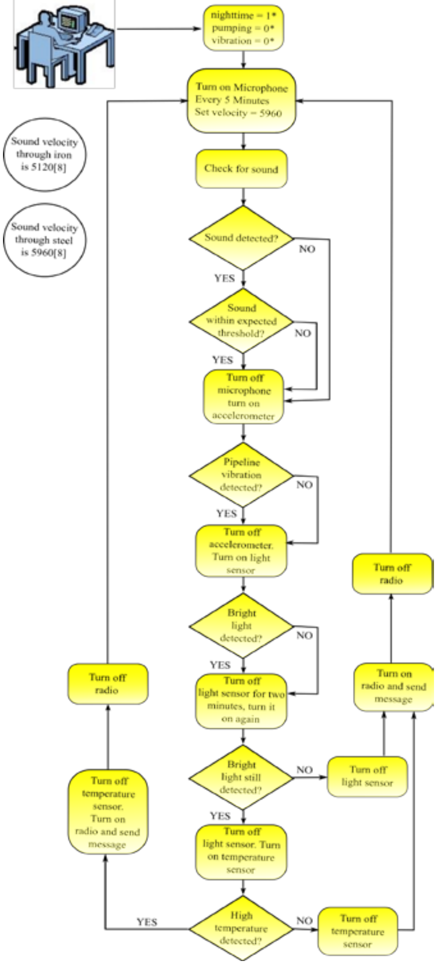

nighttime = 1*
pumping = 0*
vibration = 0*
Turn on Microphone
Every 5 Minutes
Set velocity = 5960
Sound velocity through iron is 5120[8]
Sound velocity through steel is 5960[8]
Check for sound
Sound detected?
NO
YES
Sound within expected threshold?
NO
YES
Turn off microphone turn on accelerometer
Pipeline vibration detected?
NO
YES
Turn off accelerometer. Turn on light sensor
Turn off radio
Bright light detected?
NO
YES
Turn off radio
Turn off light sensor for two minutes, turn it on again
Turn on radio and send message
Bright light still detected?
NO
Turn off light sensor
YES
Turn off temperature sensor. Turn on radio and send message
Turn off light sensor. Turn on temperature sensor
YES
High temperature detected?
NO
Turn off temperature sensor

Figure 11. Night time mode operations use up more resources

The process flowchart above (Fig. 11) represents actions to be taken by FFD motes during the night, when pipelines are empty (that is when nothing is being pumped through them). The process flowchart also eliminates false “alerts” caused by high frequency sounds such as the chirping of a bird by checking if detected sound lead to pipeline vibration. Detecting pipeline vibrations triggers the next action which involves turning on the radio and transmitting sensor's ID to the base station. But this uses light and temperature sensors.

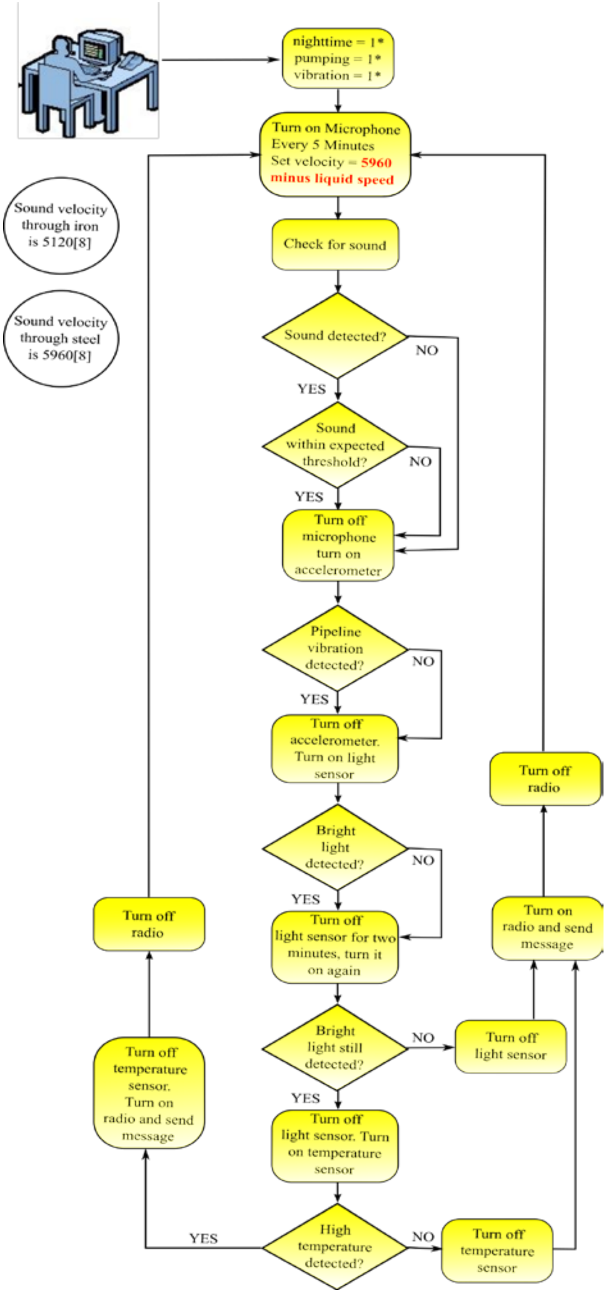

nighttime = 1*
pumping = 1*
vibration = 1*
Turn on Microphone Every 5 Minutes Set velocity = 5960 minus liquid speed
Sound velocity through iron is 5120[8]
Sound velocity through steel is 5960[8]
Check for sound
Sound detected?
NO
YES
Sound within expected threshold?
NO
YES
Turn off microphone turn on accelerometer
Pipeline vibration detected?
NO
YES
Turn off accelerometer. Turn on light sensor
Turn off radio
Bright light detected?
NO
YES
Turn off radio
Turn off light sensor for two minutes, turn it on again
Turn on radio and send message
Bright light still detected?
NO
Turn off light sensor
YES
Turn off temperature sensor. Turn on radio and send message
Turn off light sensor. Turn on temperature sensor
YES
High temperature detected?
NO
Turn off temperature sensor

Figure 12. Vibration algorithm will change once liquid is pumped through pipeline

Figure 12 above represents algorithm to execute during the night, when pipeline is in use (that is when crude or related products are being pumped through pipelines). But this also uses light and temperature sensors.

IV. SIMULATION RESULT

The pipeline monitoring solution was developed using TinyOS 2.1.2 on Ubuntu 14.04 LTS. TinyOS Yeti2 plugin for Eclipse IDE was installed to enable TinyOS software development under Eclipse 3.8. During the course of testing, it was discovered that TOSSIM [9] (TinyOS Simulator), cannot simulate certain hardware features (such as microphone). Hence, Berkley University's Avrora [10] (The AVR Simulator and Analysis Framework) was downloaded and installed from [16].

Another limitation discovered during the course of simulating the solution is the inability of available simulators to use hardware available on the host computer to emulate certain features of the mote. For example, the computer's microphone should be used during simulation when a call is made to use Micaz's acoustic microphone. To overcome this and other limitations, flashing of Micaz's led was used to simulate the turning on and off of microphones and other sensors.

The solution does not seek to modify the behavior of B-MAC. Rather, it simply recommend keeping the radio on FFD turned off until needed.

Project workability is the primary goal of using wireless sensors to monitor pipelines in Nigeria. Nonetheless, simulating energy dissipation rate of deployed motes goes a long way to guide future power pack design and deployment plans.

The energy dissipation graphs of the simulation are shown below (Figures 13 and 14). Both solutions dissipate equal energy during FFD transmissions. However, our proposed solution (Figure 14) will dissipate less energy overtime since radio usage (that is turning the radio on and off) is predetermined by the presence of sound.

Nonetheless, periodic turning on of mote’s microphone, accelerometer and temperature sensors will most likely negates intended energy gained from periodic usage of FFD’s radio.

Our proposed solution reduced collusion and lost as a result of delays which can be attributed to the need to verify detected sound before reporting.

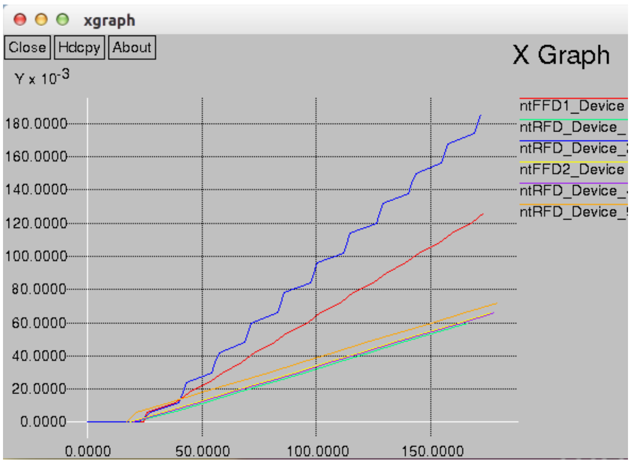


Figure 13. Normal transmission energy dissipation graph using short delays.

ISBN: 978-1-61208-503-6

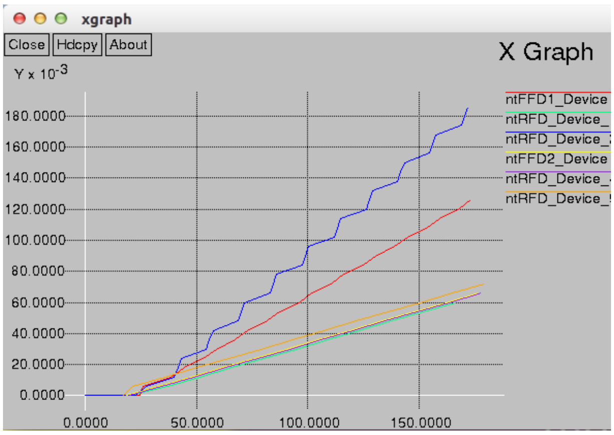


Figure 14. Energy transmission graph of our proposed solution

V. CONCLUSION AND FUTURE WORK

This paper has proposed the use of wireless sensors to monitor acoustics, vibrations and lights emanating from or around targeted pipelines. Motes are best positioned to achieve 24/7 surveillance of oil pipelines. However, this will only materialize through adequate planning and deployment strategy. Planning includes combination of hardware and software options, to boost performance and to ensure energy sufficiency.

We believe adding imaging ability will further enhance the project. This involves using concealed cameras which can communicate with Micaz, Mica2 and IRIS motes by capturing and sending low quality images of areas which Base station operators wish to see.

Moreover, additional work needs to be done on mote simulators. Especially in the area of emulating mote hardware by integrating into host's devices. For example, a call to a mote to turn on its microphone should equally turn on the microphone of the PC on which the mote is executing. Avrora simulator returns identical energy consumption values for yellow, green and blue LEDS during simulation, hence it was impossible to simulate light sensor using the three available LEDS. Finally, due to a tight budget, we could not deploy motes in a physical environment, we therefore, recommend that further research work on this experiment should be conducted using methods outlined in this project.

REFERENCES

[1] M. F. F. Bin Ismail and Wai Yie "Acoustic Monitoring System Using Wireless Sensor Networks" International Symposium on Robotics and Intelligent Sensors, 2012, pp. 2-7.

[2] A. M. Sadeghion, N. Metje, D. N. Chapman, and C. J. Anthony "Smartpipes: Smart Wireless Sensor Networks for Leak Detection In Water Pipelines" Journal of Sensor and Actuator Networks, February 2014, pp. 1-15.

[3] O. Diallo, J. J. P. C. Rodrigues and M. Sene, "Real-time data Management on wireless sensor networks: A survey" Journal of Network and Computer Applications, www.elsevier.com/ locate/jnca December 2011, pp.2 – 8.

[4] G. Han, X. Jiang, A. Qian, J. J. P. C. Rodrigues, and L. Cheng, "A Wireless Comparative Study of Routing Protocols of Heterogeneous Sensor Networks", Research Article, June 2014, pp. 1-3.

[5] L. M. L. Oliveira, J. J. P. C. Rodrigues, A. G. F. Elias and B. B. Zarpelão, "Ubiquitous monitoring solution for Wireless Sensor Networks with push notifications and end-to-end connectivity" 2014 pp. 1 - 2.

[6] K. Lin, J. J. P. C. Rodrigues, H. Ge, Naixue Xiong, and X. Liang "Energy Efficiency QoS Assurance Routing in Wireless Multimedia Sensor Networks", IEEE Systems Journal, Vol. 5, December 2011 pp.1-3.

[7] V. N. G. J. Soares and J. J. P. C. Rodrigues, "Cooperation in DTN-Based Network Architectures" V2-05, April 2011, pp. 103 – 107.

[8] M. Shilpa, Tamanna, and K. Mukesh "A Comparative Study of Power Aware Routing Protocols of Ad Hoc Network" International Journal of Computer Applications (IJCA), 2011, pp. 1 – 5.

[9] S. A. Ahlam, and A. Manal," Medium Access Control Protocols for Wireless Sensor Networks Classifications and Cross- Layering" Science Direct, Procedure Computer Science, www.ScienceDirect.com, ICCMIT, 2015, pp. 2-13.

[10] N. Bhavana, S. Anuradha, K. Sanjay, and P. Vinod "Energy Efficient MAC Protocols for Wireless Sensor Networks: A Survey" Computer Science and Engineering Survey Vol.2, No. 3, August 2011, pp. 122-129.

[11] E. Romero, A. Araujo, J. Blesa, and O. Nieto-Taladriz "Developing Cognitive Strategies for Reducing Energy Consumption in Wireless Sensor Networks" The Second International Conference on Advances in Cognitive Radio, COCORA 2012, pp. 64 – 65.

[12] L. M. L. Oliveira and J. J. P. C. Rodrigues, "Wireless Sensor Networks: a Monitoring" Journal of Communications, April 2011, Vol. 6, No. 2, pp. 3-16.

[13] M. Alnuem" Performance Analysis of Node Placement in Linear Wireless Sensor Networks" Journal of Emerging Trends in Computing and Information Sciences, January 2014, Vol. 5, No. 1, pp.1 – 8.

[14] Intrinsic Solutions: MEMSIC Wireless Modules http://www.intrinsic.in/Products/Memsic-WirelessModules.aspx

[15] Sound Frequency and Wavelength Calculator http://www.1728.org/freqwavf.htm

[16] The AVR Simulator and Analysis Framework, Berkley University http://compilers.cs.ucla.edu/avrora/release.html

[17] L. Luo, Q. Cao, C. Huang, T. Abdelzaher, John A. Stankovic, and M. Ward, "EnviroMic: Toward Cooperative Storage and Retrieval in Audio Sensor Networks", 2009, pp. 1- 22

[18] J. Kim, G. Sharma, N. Boudriga, and S. S. Iyengar "SPAMMS: A Sensor-based Pipeline Autonomous Monitoring and Maintenance System" IEEE Explore, 2010, pp.2-11.

ISBN: 978-1-61208-503-6

Fast and Memory Efficient NFA Pattern Matching using GPU

Yeim-Kuan Chang and Yu-Hao Tseng
Department of Computer Science and Information Engineering
National Cheng Kung University
Tainan, Taiwan
Email:ykchang@mail.ncku.edu.tw

Abstract—**Network intrusion detection system (NIDS) is mainly designed to monitor the malicious packets spreading on the Internet. With pre-defined virus signatures called patterns, NIDS can find out whether these pre-defined patterns exist in the packet's payload. GPU can be useful to effectively accelerate pattern matching process due to abundant parallel hardware threads. In this paper, we propose a constrained NFA (CNFA) scheme to store complex regular expressions in limited memory of GPU effectively. CNFA is constructed from the original NFA based on the subset construction algorithm that converts NFA to DFA. Compared to original NFA and DFA, CNFA imposes a constraint that each state can only have at most two transitions (self-loop and non-self-loop) for each character. Based on our experimental results, CNFA can achieve the performance of about 100 Gbps for one of the tested rule sets on GPU. Also, CNFA only needs 18% of memory needed in iNFAnt. In addition, CNFA can be used for more complex rule sets that is not possible to be implemented in iNFAnt.**

Keywords- Deep Packet Inspection; DFA; NFA; GPU; Pattern Matching; Regular expression.

I. INTRODUCTION

Due to the popularity of the Internet, Internet traffic increases exponentially. Network security has become a significant issue because more malicious attacks, such as malwares and viruses, have spread on the Internet. Traditional protections, such as firewalls, have been inadequate to protect our computers. Instead, Network Intrusion Detection System (NIDS) has been diffusely used to maintain the security of network activities. The main task of NIDS is to examine the payload of each input packet to find out whether or not the packet contains suspicious contents based on the pre-defined rules. If there are some suspicious contents contained in the input packet, NIDS reports all occurrences of these suspicious contents associated with the matched rules.

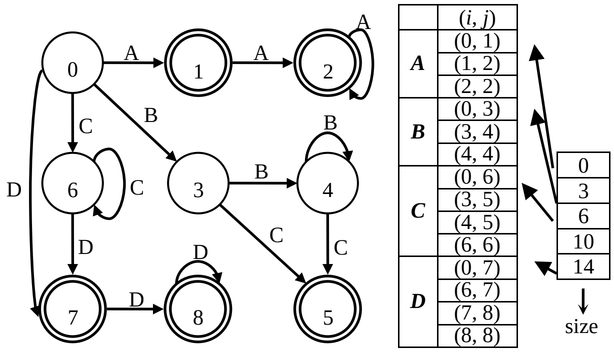
In computer science, pattern matching algorithms are used to check a given text of tokens for the presence of the constituents of some patterns. In other words, we often utilize the idea of pattern matching to develop the NIDS. According to different forms of rules, pattern matching is divided into string and regular expression matching. For regular expression matching, most people implement finite state machine, such as non-deterministic (NFA) and deterministic (DFA) finite automata, to perform the matching operations. We can first translate a regular expression into a parse tree and use one of these algorithms, which contain Thompson [10] and Glushkov [3] algorithms, to build a NFA on the basis of the parse tree. We can even transform the NFA into an equivalent DFA. With the rapid expansion of networks, traditional software-based approaches are not able to satisfy these demands. A lot of researches attempt to improve the performance of pattern matching on different devices. For example, Baker and Prasanna [11] proposed variants version of KMP algorithm and implement on FPGA. Zha and Sahni [12] and Lin et al. [13] proposed a Parallel Failureless-AC (PFAC) algorithm that uses Computer Unified Device Architecture (CUDA) to implement modified version of AC algorithm on GPU which NVIDIA corporation produces. PFAC is the simple version of AC algorithm but suitable for GPU. PFAC effectively streamlines AC algorithm by utilizing massive threads of GPU. The main idea of PFAC is to assign each thread to process input stream at the corresponded position of stream. Each thread accesses the same goto function whose initial state has no self-loop. In the above hardware, GPU has high scalability and low overhead. When we choose CUDA as our programing language, implementing General-purpose computing on graphics processing units (GPGPU) becomes an easy work.

In this paper, we propose our scheme which decreases memory consumption of the original NFA and utilizes SIMT (Single Instruction Multiple Thread) of GPU to accelerate NFA's searching procedure to get the better performance. In our experiment, we can reach performance around 6 Gbps at worst case.

The rest of the paper is organized as follows. Section II describes the related work. In Section III, gives a detailed description of the proposed scheme. Section IV outlines the implementation on GPU. Section V presents the experimental results that are compared to the existing GPU implementation called iNFAnt [1]. Finally, our conclusions are stated in Section VI.

II. RELATED WORK

In this paper, we focus on regular expressions that can specify a finite set of strings mainly used in pattern matching. Traditional software-based approaches are unable to meet the performance requirement of the NIDS. Several researches have attempted to improve the performance by using GPU. There is a GPU-based parallel regular expression matching engine, iNFAnt [1]. iNFAnt adopts NFA to support a very large complex rule set that are otherwise hard to solve. iNFAnt is explicitly designed and developed for running on



	(*i*, *j*)
A	(0, 1)
	(1, 2)
	(2, 2)
B	(0, 3)
	(3, 4)
	(4, 4)
C	(0, 6)
	(3, 5)
	(4, 5)
	(6, 6)
D	(0, 7)
	(6, 7)
	(7, 8)
	(8, 8)

(a) NFA transition graph.

(b) Transition table with an ancillary table.

Figure 1. Character-first representation in iNFAnt for pattern "(A+|B+C|C*D+)" and Σ = {A, B, C, D}.

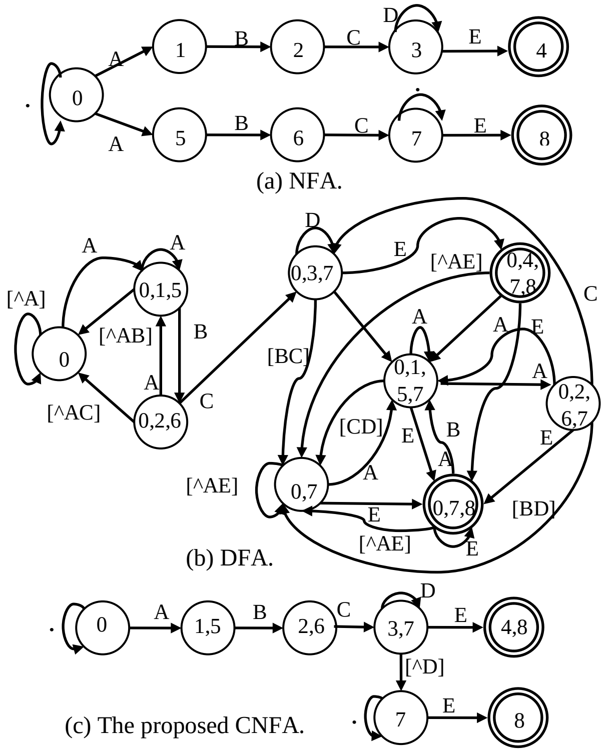
GPU consisting of a large number of threads. This parallelism is exploited to handle NFA and to process multiple packets at once, thus get better performance.

Compared to traditional NFA, iNFAnt adopts a character-first representation for state transition graph. The character-first representation keeps a list of transitions that will be triggered by each of the 256 characters. This list can grow very large so it must be stored in global memory of GPU, together with an ancillary data structure that records the index in character-first transition table for the first transition of each character in order to perform easy random lookups. Figure 1 illustrates an example of iNFAnt.

III. PROPOSED SCHEME

Pattern matching for regular expressions (RegEx) patterns is performed by searching a finite state automata (FSA) built from these patterns. Researchers are familiar with non-deterministic (NFA) and deterministic (DFA) finite automata. Automata theory confirms that both NFA and DFA are true in terms of expressiveness, but their practical properties like memory requirement and number of active states are much different. According to automata theory, each state in NFA may transit to zero or more states after processing an input character. Furthermore, each state in NFA may also transit to zero or more states without processing any input character, which we call ε-transition. Different from NFA, each state in DFA transits to only one state for an input symbol. DFA is faster than NFA because only one active state exists in any cycle. However, DFA is less memory-efficient than NFA because it requires a lot of memory to store the transition table. NFA suffers from a higher cost to traverse many states per input character but it requires much less memory than DFA. For some complicated regular expressions, it may not be possible to build the corresponding DFAs because the required memory may exceed the amount of memory that a computer can support. In order to store large RegEx sets in a scant amount of memory, we choose the architecture of NFA.

Our proposed scheme is inspired by the subset construction algorithm that converts NFA to DFA. As we know that all NFAs can be converted into equivalent DFAs by using the subset construction algorithm [2]. It is well known that complex syntaxes like ".*" and "[^\r\n]*" in RegEx lead to so-called state space explosion in DFA because a state in DFA is associated with a subset of states in NFA and most subsets contain the NFA states that are originated from these complex syntaxes. One of the advantages of subset construction algorithm is that many different states generated from the same prefix of different rules are merged and so some different transitions labeled with the same character are merged into the same transition. Consider two rules "ABCD*E" and "ABC.*E" whose NFA and DFA are shown in Figure 2. Transitions (state 0 → state 1) and (state 0 → state 5) in NFA are transformed into the transition (state {0} → state {0, 1, 5}) in DFA. The reason is that these two patterns have the same prefix "A" and thus reduces some redundant states and transitions in NFA. Obviously, the DFA in Figure 2(b) is more complex than the NFA in Figure 2(a). States 0 and 7 in NFA exist in most subsets of DFA due to ".*" syntax. This is the disadvantage that makes the number of DFA states blow up. Besides, we also observe that states 1 and 5 (or 2 and 6) in NFA exist in the same subsets of DFA. Reducing redundant states can mitigate the process of updating active states in NFA. And less transitions in NFA can lead to a better throughput. In order to utilize the observations described above, we propose a new NFA called constrained NFA (CNFA) that considers the regular expressions containing the syntax of ".*" and counters.



(a) NFA.

(b) DFA.

(c) The proposed CNFA.

Figure 2. Finite State Automata for {ABCD*E, ABC.*E}.

To show the proposed CNFA and original NFA, we use a simple rule set example containing two rules, "ABCD*E" and "ABC.*E", in Figure 2 and explain the difference between them. Assume that character set only includes A, B,

TABLE 1. DEFINITIONS OF CNFA CONSTRUCTING ALGORITHM.

notation	Description
S_i ($S_{i'}$)	State *i* in NFA (State *i'* in CNFA)
Φ(*i'*)	NFA states associated with state *i'* in CNFA
Σ	The character set
GroupNum	# of tuples in *StateClosureGroup*
StateClosureGroup	NFA states reachable from one of the NFA states in Φ(*i'*) are divided into *GroupNum* subsets based on repetitions. These *GroupNum* subsets are put into *StateClosureGroup* which is a *GroupNum*-tuple list.

C, D and E. The proposed CNFA is shown in Figure 2(c). It is obvious that the proposed CNFA has fewer states than NFA. Because we merge some states in NFA, we can get multiple matched rules in final states of the proposed CNFA.

We will first illustrate the procedure of converting NFA to CNFA. Table 1 lists some definitions of our CNFA constructing algorithm to help us understand the converting procedure. Figure 3 shows the pseudo code of the proposed CNFA construction algorithm. Figure 4 show the NFA and CNFA for rule set {ABCD*E, ABC.*E, CDEA+C, CDE.*C} and Σ = {A, B, C, D, E}. Table 2 shows the complete list of Si' and the associated Φ(i') Figure 4(b). For example, S0 is the initial state in NFA, S5' denotes that the state 5 in CNFA is equivalent to a set of corresponding NFA states where Φ(5') = {S3, S7}. According to line 1 of the pseudo code, we add the initial state of the proposed CNFA. Because NFA has no ε-transitions, Φ(0') is set to {S0}. From lines 2-15, we process each CNFA state Si' and add accessible transitions labeled with the character α from Si' to Stmp' that is the temporary state of CNFA during the conversion. Unlike the subset construction algorithm [2], we divided the process of computing accessible transitions from a state to its next state into two parts, the self-loop transition and the non-self-loop transition for each state in Φ(i'). In lines 4-8, we add an accessible non-self-loop transition Si' to Stmp' labeled with character α. In lines 9-13, the same codes are performed for self-loop transition. In line 4, function Extract-NonSelfLoop-States(Φ(i'), α) collects all the states j from non-self-loop transitions i → j with label α in the original NFA for i ∈ Φ(i'). In other words, it computes a set of NFA states that can be reached from one of the NFA states in Φ(i') by a non-self-loop transition with label α. Similarly, function Extract-SelfLoop-States(Φ(i'), α) collects all the states j (i.e., Φ(tmp')) from self-loop transitions i → j with label α in the original NFA for i ∈ Φ(i'). As a result, we obtain the full table of the proposed CNFA except the information of final states. Therefore, in line 16-20, we mark the final states of CNFA based the information of final states in the original NFA. Here we will give a graphic example of converting NFA to CNFA in Figure 4 by using rule set containing rules "ABCD*E", "ABC.*E", "CDEA+C" and "CDE.*C". Notice that NFA is constructed according to Glushkov algorithm [3]. In this paper, we will also use the character-first format to store the transition table of the proposed CNFA.

A. Compression by Default State

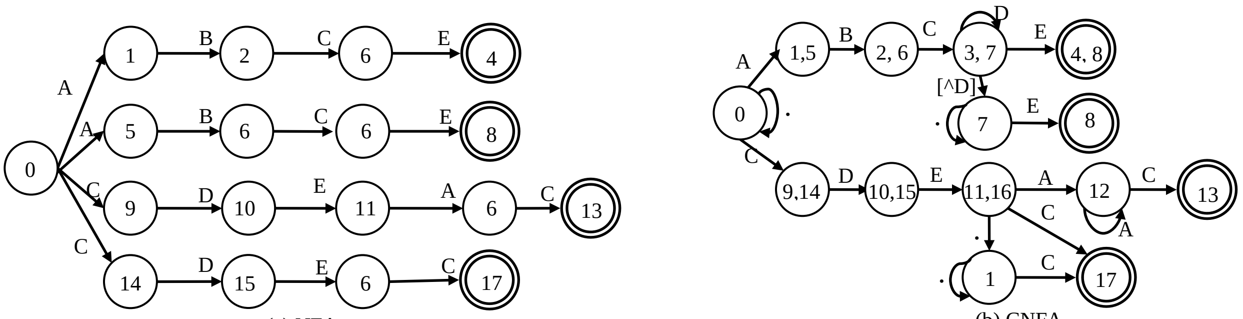
Before describing the details of the proposed compression schemes, we analyze the number of transitions for the NFA states based on Snort534 [4]. We observe that most characters have a large constant number of transitions. Every character appears to be the transition symbol for at least 200 transitions. In other words, a source state has more different transitions to the same destination state. This appearance takes place due to overlapping syntaxes such as "." and "[^\r\n]". As a result, based on character-first data structure for transition table, more memory is required. In order to reduce the number of transitions per symbol for character-first for transition table, we record default transition for each state by using a simple traditional state-first transition table. Take the CNFA in Figure 4(b) as an example. The character-first transition table is shown in Figure 5(a). We build a default state table (DST) in Figure 5(b) including four fields, the default next state of each state, default character and don't care character of the default transition, and the compliment flag. If don't-care character bit is 0, the default transition follows the default character. Otherwise, the default transition is unconditional, i.e., the default transition is taken no matter what the input character is. If the complement flag is set to 1 and the default character is C, the default transition will follow the symbol ^C (i.e., any character other than C).

```
Convert_NFA_to_CNFA (NFA)
01 CNFA = {0'} and Φ(0') = {$S_0$}; tmp' = 1;
02 for each non-processed state i' in CNFA {
03    for each α in Σ {
04        Φ(tmp') = Extract-NonSelfLoop-States(Φ(i'), α);
05        if ($S_{tmp'}$ ∉ CNFA) CNFA = CNFA + $S_{tmp'}$; tmp'++;
06        add a transition $S_{i'}$ to $S_{tmp'}$ labeled with α;
07        Φ(tmp') = Extract-SelfLoop-States(Φ(i'), α);
08        if ($S_{tmp'}$ ∉ CNFA) CNFA = CNFA + $S_{tmp'}$; tmp'++;
09        add a transition $S_{i'}$ to $S_{tmp'}$ labeled with α;   }
10 }
11 for each state i' in CNFA
12     if (any $S_i$ ∈ Φ(i') is a final state in the NFA)
13         Set $S_{i'}$ as final state in CNFA;
14 return CNFA;
```

Figure 3. Pseudo code of constructing CNFA.

B. Counter

As far as we know, counter is used to solve repetitions of RegEx. In terms of data structure, we store the information of repetition in a table which keeps a list of counter pairs (min, max) for every state. Therefore, the proposed CNFA construction algorithm has to be modified. As shown in Figure 6(a), the reachable NFA states, *Φ(tmp')*, from any state in *Φ(i')* returned by functions *Extract-SelfLoop-States*() and *Extract-NonSelfLoop-States*() need further process to consider the repetition conditions. What we do is to divide *Φ(tmp')* into several groups based on the repetition conditions performed by function *UpdateCNFA*(). Lines 2-5 of *UpdateCNFA*() in Figure 6(b) are responsible for grouping based on the repetition conditions. *GroupRepState*() function divides Φ(tmp') into several groups when Φ(i') of current Si' does not contain a repetition state of NFA. *IdentifyLeaveRep*() function that is similar to *GroupRepState*() divides *Φ(tmp')* into two groups, one for the CNFA state leaving the repetition and the other for the CNFA state continuing the repetition when current Si is a repetition state.



(a) NFA.

(b) CNFA.

Figure 4. NFA and CNFA for Rule Set = {ABCD*E, ABC.*E, CDEA+C, CDE.*C} and Σ = {A, B, C, D, E}.

	A								B						C										D						E							
src	0	0	5	6	6	7	9	10	0	1	5	6	7	9	0	0	3	5	6	6	7	9	9	10	0	2	5	6	7	9	0	4	5	5	6	7	7	9
dst	0	1	7	9	10	7	9	10	0	3	7	9	7	9	0	2	5	7	9	11	7	9	11	13	0	4	5	9	7	9	0	6	7	8	9	7	12	9

A	B	C	D	E	-
0	8	14	24	30	38

→ Total Size of TT

(a) The character-first transition table.

Transition Table

	A		B	C				D	E	
src	0	6		0	6	9	10	5	5	7
dst	1	10		2	11	11	13	5	8	12

A	B	C	D	E	-
0	2	2	6	7	9

→ Size of TT

Default State Table (DST) of size |DST| = 14

State #	***0***	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***		***13***
Default State	0	3	4	5	6	7	9	7	14	9	10	14	14		14
Default Char	n/a	B	D	C	E	D	n/a	n/a	n/a	n/a	A	n/a	n/a		n/a
Don't care Char	1	0	0	0	0	0	1	1	0	1	0	0	0		0
Compliment Flag	0	0	0	0	0	1	0	0	0	0	0	0	0		0

(b) The character-first transition table enhanced by default state table.

Figure 5. The complete data structure for Figure 4(b).

IV. GPU IMPLEMENTATIONG

In this section, we will emphasize how to parallelize the general purpose procedure. First, all threads in the same block initialize and update the active state list together. Second, we also exploit parallelism that GPU offers to accelerate. We select valid transitions for the current symbol and all threads in the same block averagely sharing the workloads. Similarly, we use parallelism to speed up the process that access Default State Table when the design architecture contains Default State.

According to different requirements, we first consider that transition table, the default state table and then counters should be stored in suitable type of memory space. Because these tables need larger memory space and every task reads the same data structure, we choose global memory and texture memory that can be read by all threads on GPU. How large is texture memory is dependent on the size of global memory and texture memory is cached on chip. In some situations, texture memory will provide higher effective bandwidth by reducing memory requests to off-chip DRAM. So we store our tables in texture memory.

Furthermore, we have to find out memory space suitable for input streams. If input streams assigned in a block can be stored in enough shared memory, we will choose this storing mode. Because shared memory is faster than other memory spaces except register. And the famous problem of using shared memory is bank conflict. In order to get higher bandwidth, shared memory is divided into memory modules which are the same memory size when parallelizing memory accesses. The memory module is named as bank and different banks can be accessed at the same time. When all 16 threads of half-warp access the same memory address in the same bank, shared memory adopt the broadcast mode to respond requirements of half-warp. So we don't have bank conflict because all threads on the GPU read a character of the input stream from shared memory at every cycle.

V. EXPERIMENT RESULTS

Our experiments are based on three rule sets and we compare throughput and memory consumption with iNFAnt [1]. Moreover, we show the comparison of throughput and memory consumption with different compressed schemes. And also we show that the influence on throughput by workload per block.

All experiments were performed using a 4-core Intel Core i5-650 machine running at 3.2 GHz with 8 GB of RAM. GPU tests were implemented on the same platform equipped with one graphic card which is NVIDIA GeForce GTX 770. The GPU has 2 GB of RAM and 8 multiprocessors clocked at 1.11 GHz, and its compute capability is version 3.0. Though the GPU supports PCI-E 3.0, the motherboard on our PC supports only PCI-E 2.0. Finally, we install Ubuntu 12.04.4 LTS x64 on the PC.

In our experiments, we use 2 rule sets which is taken from iNFAnt [1] and an additional rule set to finish our experiments. The first rule set, *Snort534*, taken from [4] is composed of 534 regular expressions. *Snort534* can be partitioned into subsets that share an initial part while the tails differ. The second rule set, *L7-filter*, is from the L7 traffic classifier [5] and consists of 115 regular expressions. *L7-filter* is a very complex and irregular rule set where no

```
NFA_to_CNFA(NFA_in)
NFA_out = {}
Set the initial state $S_{0'}$ in NFA_out and let $\Phi(0') = \{S_0\}$;
for each non-processed state $i'$ in NFA_out {
    for each $\alpha$ in $\Sigma$ {
        $\Phi(tmp') = ExtractSelfLoopStates(\Phi(i'), \alpha)$;
        $UpdateNFA_{out}(NFA_{out}, i', \Phi(tmp'), \alpha)$;
        $\Phi(tmp') = ExtractNonSelfLoopStates(\Phi(i'), \alpha)$;
        $UpdateNFA_{out}(NFA_{out}, \Phi(tmp'), \alpha)$; }
}
for each state $i'$ in NFA_out
    if (any $S_i \in \Phi(i')$ is a final state in the NFA_in)
        Set $S_{i',\Phi(i')}$ as one final state of the NFA_out;
return NFA_out;
```

(a) Algorithm Convert_NFA_to_CNFA_counter.

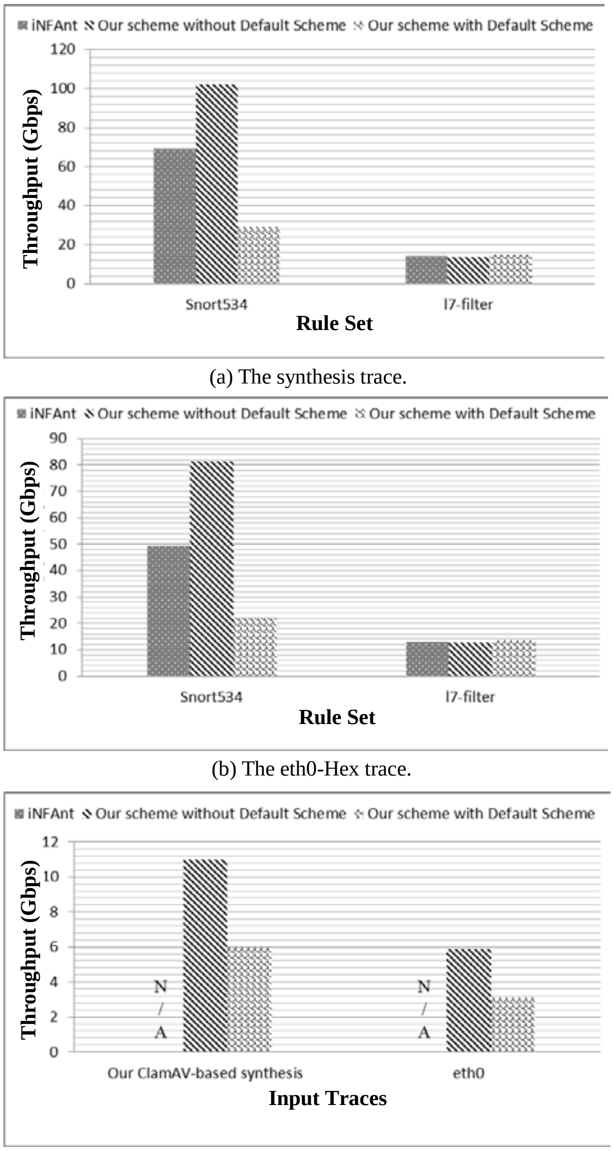
```
UpdateNFA_out(NFA_out, $i'$, $\Phi(tmp')$, $\alpha$)
StateClosureGroup ={};
if ($S_{i',\Phi(i')}$ is a repetition state)
    StateClosureGroup = IdentifyLeaveRep($\Phi(tmp')$);
else
    StateClosureGroup = GroupRepState($\Phi(tmp')$);
for each set $j$ in StateClosureGroup {
    set temp state $S_{tmp',\Phi(tmp')}$, where $\Phi(tmp')$ = set $j$;
    if ($S_{i',\Phi(i')}$ is a repetition state )
        for each state $S_x$ in $\Phi(tmp')$ {
            find state $S_{y'}$ in NFA_out such that $S_x \in \Phi(y')$ {
                add a $\alpha$-transition from $S_{i'}$ to $S_{y'}$ ;
                $\Phi(tmp') = \Phi(tmp') - \{S_x\};$}
        if $\Phi(tmp')$ is not empty {
            create a new state $S_{tmp',\Phi(tmp')}$ in NFA_out;
            add a $\alpha$-transition from $S_{i'}$ to $S_{tmp'}$; }
    else
        if ($S_{tmp',\Phi(tmp')}$ does not exust in NFA_out)
            create a new state $S_{tmp',\Phi(tmp')}$ in NFA_out
        add a $\alpha$-transition from $S_{i'}$ to $S_{tmp'}$;
}
```

(b) Algorithm *UpdateNFA*$_{out}$.

Figure 6. Pseudo code of the proposed CNFA construction.

special properties or common prefixes can be exploited. Because of these same rule sets, these comparisons between iNFAnt and the proposed CNFA deserve to be a reference. Finally, we also take an additional rule set which is Emerging Threats [6] Open optimized for *Suricata* [7] because previous two rule sets don't have complex regular expressions with repetitions. Table 4 shows feature of these rule sets.

We compare the memory consumption of the proposed CNFA with iNFAnt [1] by using different rule sets. In addition, we also show the difference between these compressed schemes we proposed. Table 5 shows the comparison results for *Snort534*, *L7-filter*, and *Suricata*. Because there is no syntax of repetition in *Snort534*, *L7-filter*, the comparison has no experimental data of Counter scheme. We find out that CNFA decreases around 60% of memory consumption needed by iNFAnt for *Snort534*, but less than 1% of memory needed by iNFAnt for *L7-filter*. The reason is that *Snort534* has many common prefixes between different rules but *L7-filter* is a complex and irregular rule set where no special properties or common prefixes can be utilized. Compared to *Snort534* and *L7-filter*, rule set *Suricata* has complex repetitions. Due to complex repetition conditions, the complete data structures of iNFAnt [1], as well as CNFA without Counter scheme cannot be built for *Suricata*. So Table 5(c) shows only experimental data of CNFA with Counter scheme and CNFA with Counter scheme and the default state table.



(a) The synthesis trace.

(b) The eth0-Hex trace.

(c) Performance of Suricata with different input traces.

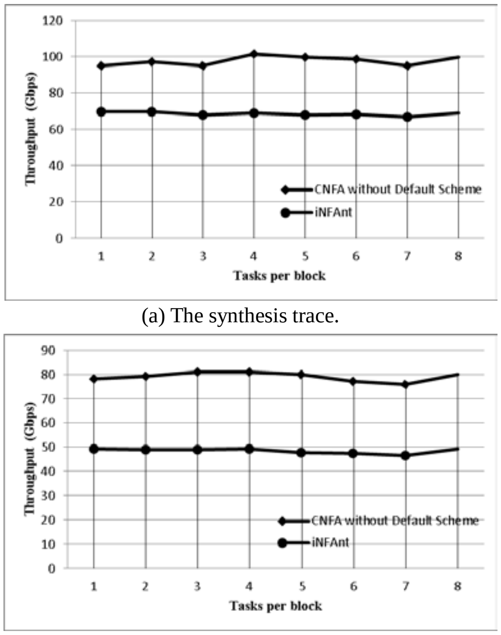
Figure 7. Performance with different input traces.

In Figure 7, we show the throughputs of iNFAnt compared with CNFA and CNFA with Default State Table. The difference between these two figures is that one uses our ClamAV-based [8] synthesis and the other utilizes eth0 taken from Defcon [9]. In Figure 7(c), we use *Suricata* to build our finite state machine, but the data structure of iNFAnt can't be built due to insufficient memory on the device. So we only show the performance of CNFA with counter scheme.

Finally, we test iNFAnt [1] and our proposed CNFA by controlling the number of tasks per block. We test the two input traces with rule set Snort534. Figure 8 shows the throughputs. We discover that increasing the number of tasks doesn't evidently accelerate the searching speed of iNFAnt [1]. The proposed CNFA gets most performance gain when the number of tasks is four.

TABLE 4. DETAILS OF RULE SETS

Snort534 [4]	*L7-filter* [5]	*Suricata* [6]
534	115	1195
common prefixes	complex, irregular, and no common prefixes	similar to snort and complex repetition



(a) The synthesis trace.

(b) The eth0-Hex trace.

Figure 8. Performances of different number of tasks.

VI. CONCLUSION

In this paper, we proposed a scheme on GPU with efficient utilization of memory space to avoid the so-called state space explosion. The main for searching is that we assign each block on GPU to process appropriate amount of tasks. And we utilize massive amount of threads to accelerate the process of finding possible transitions to next states. Compared to iNFAnt [1], our scheme does not increase the complexity of NFA searching but accelerate the searching procedure because it can decrease the number of states for most rule sets. And we assign each thread to be responsible for number of tasks and avoid latency of block switch.

By utilizing the same rule set, our method can reach 101.94 Gbps for one of the tested rule sets. With our compression scheme, we need 18% of iNFAnt's memory usage with the same rule set. Besides, we proposed the architecture for counters to slow down state space explosion which is caused by repetitions. The proposed CNFA scheme obviously slows down our performance and we can construct the complete search data structure for more complex rule sets that is not possible for iNFAnt.

TABLE 5. MEMORY (KB) CONSUMED by iNFANT, CNFA, AND CNFA WITH DEFAULT STATE (denoted by CNFA_{de}).

	iNFAnt	**CNFA**	**CNFA_{de}**
# of states	14,566	9,696	9,696
# of transitions	160,657	59,869	3,225
TT	627.6	233.9	12.6
DST	N/A	N/A	74
Match Table	56.9	2.1	2.1
Match List Flag	N/A	37.9	37
Total	685.5	274.9	125.7
Ratio over iNFAnt	x1.0	x0.40	x0.18

(a) *Snort534 with no repetition syntax.*

	iNFAnt	**CNFA**	**CNFA_{de}**
# of states	6,123	6,006	6,006
# of transitions	1,400,594	1,397,104	1,397,104
TT	5471.1	5427.2	914.4
DST	N/A	N/A	295.8
Matched Table	23.9	23.5	23.5
Matched List Flag	N/A	3.0	3.0
Total	5496.0	5454.7	1236.8
Ratio over iNFAnt	x1.0	x0.99	x0.23

(b) *L7-filter with no repetition syntax.*

	CNFA	**CNFA_{de}**
# of states	27,574	27,574
# of transitions	423,501	41,592
TT	1653.8	162.5
DST	N/A	353.3
Repetition Table	107.7	107.7
Matched Table	7.4	7.4
Matched List Flag	107.7	107.7
Total	1876.6	738.5

(c) *Suricata with repetition syntax.*

REFERENCES

[1] N. Cascarano, P. Rplando, F. Risso, and R, Sisto, "iNFAnt: NFA Pattern Matching on GPGPU Devices," ACM SIGCOMM Computer Communication Review, vol. 40 Num. 5, pp. 21-26, 2010.

[2] J. C. Marrtin, "Introduction to Languages and the Theory of Computation." McGraw Hill, pp.108, 2010

[3] V-M. Glushkov, "The abstract theory of automata." Russian Mathematical Surveys 16-5, pp.1–53, 1961.

[4] M. Becchi, C. Wiseman, and P. Crowley, "Evaluating Regular Expression Matching Engines on Network and General Purpose Processors," the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, 2009. pp. 30-39

[5] L7-filter, "Application Layer Packet Classifier for Linux". [Online]. Available. http://l7-filter.sourceforge.net/ 2013.06.05

[6] Emerging Threats. [Online]. http://emergingthreats.net/

[7] Suricata. [Online]. http://suricata-ids.org/ 2016.06.20

[8] ClamAV. [Online]. http://www.clamav.net/ 2016.05.03

[9] Defcon. [Online]. Available : http://www.defcon.org/ 2016.4.7

[10] K. Thompson, "Programming Techniques: Regular expression search algorithm." Communications of the ACM Volume 11 Issue 6, pp. 419-422, 1968.

[11] Z. K. Baker, and V. K. Prasanna, "Time and Area Efficient Pattern Matching on FPGAs," Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays, pp.223-232, 2004.

[12] X. Zha, and S. Sahni, "GPU-to-GPU and Host-to-Host Multipattern String Matching On A GPU," IEEE Transactions on Computers, vol.62, pp.1156-1169, 2013.

[13] C.-H. Lin, C.-H. Liu, L.-S. Chien, and S.C. Chang, "Accelerating Pattern Matching Using a Novel Parallel Algorithm on GPUs," IEEE Transactions on Computers, 62 (10), pp.1906-1916, 2013.

Performance Anomaly in Download TCP Flows Over IEEE 802.11n Wireless LAN

Yoshiki Hashimoto, Masataka Nomoto, Celimuge Wu, Satoshi Ohzahata, and Toshihiko Kato
Graduate School of Information Systems
University of Electro-Communications
Tokyo, Japan
e-mail: hys3224@net.is.uec.ac.jp, noch@net.is.uec.ac.jp, clmg@is.uec.ac.jp, ohzahata@is.uec.ac.jp, kato@is.uec.ac.jp

Abstract— **The performance anomaly is one of well-known performance problems in IEEE 802.11 wireless LANs (WLANs). It reduces the throughput of all stations managed by one access point when some of them use low data rates even if the others use high rates. In the recent WLANs, such as 802.11n WLAN, providing higher data rates than the legacy ones, the performance degradation due to the performance anomaly may give larger impacts. In the previous paper, we showed the evaluations of the performance anomaly for UDP and TCP flows over 802.11n WLAN. The results show that, although the performance anomaly occurs for UDP flows, the situation is different for TCP flows. This paper presents more detailed experimental performance study on the performance anomaly for download TCP flows analyzing the throughput, the congestion window size (cwnd) and the round trip time (RTT). It concludes that, although the throughput degrades where there are low data rate stations, the so called performance anomaly does not occur in download TCP flows.**

Keywords- WLAN; IEEE802.11n; Performance Anomaly, TCP flows.

I. Introduction

Recently, a variety of equipment based on IEEE 802.11 WLAN standard [1], such as smart phones, tablets and notebooks, are widely deployed. When a number of stations access to one WLAN access point, they suffer from several kinds of performance problems. Among them, the *performance anomaly* [2][3] is a well-known problem. When some stations are located far from their access point and others are near it, the performance of the near stations is degraded to that of far located stations. This is caused by the fair assignment of channel access based on the *carrier sense multiple access with collision avoidance* (*CSMA/CA*) principle, and the multiple Media Access Control (MAC) level data rate support. Those allow stations with low bit rate to capture the channel for a long time, and it penalizes other stations with higher data rates.

Nowadays, 802.11n [1] is one of most widely adopted IEEE WLAN standards. It establishes high speed data transfer using the higher data rate support (e.g., 150 Mbps), the frame aggregation in Aggregated MAC Protocol Data Unit (A-MPDU) and the Block Acknowledgment mechanism. In spite of those improvements, 802.11n standard does not resolve the performance anomaly. So, the performance degradation by the performance anomaly will give larger impacts than the legacy standards.

There are a few papers describing the performance anomaly in IEEE 802.11n WLANs. Abu-Sharkh and Abdelhadi [4] reports that the performance anomaly still exists in 802.11n WLANs. It describes the results of the upload TCP data transfer focusing on the A-MPDU function. Our previous paper [5] shows the results of examining performance anomaly in UDP and TCP download data transfer. It describes that the performance anomaly surely occurs in UDP flows, but there may be only performance degradation in download TCP flows even in near and far located stations coexist.

This paper presents more detailed experimental performance analysis on the performance anomaly for download TCP flows. The feature of our analysis is as follows.

- During a TCP flow, the time variation of the throughput, cwnd and RTT are examined in detail, instead checking their average values.
- From the cwnd and RTT values, the traffic load to the access point is estimated, and it is compared with the actual MAC level data rate.
- The experiments with two stations and with four stations are performed.
- The commercially available access point is used with installing the firmware provided by the OpenWRT project [6]. This allows us to obtain various MAC level performance metrics and to adopt different queue management schemes at the access point.

The rest of this paper consists of the following sections. Section 2 shows the experimental settings. Sections 3 and 4 describe the results of the two station and four station experiments, respectively. In the end, Section 5 gives the conclusions of this paper.

II. Experimental Settings

Fig. 1 shows the configuration of our experiment. Up to four stations (STAs) conforming to 802.11n with 5GHz band are associated with one access point, which is connected with a server through 1Gbps Ethernet. Some STAs are located at a near position to the access point, and another STA is located in various positions in the experiment.

The detailed specifications of stations and the access point are shown in Table 1. We use commercially available notebooks and access point in the experiment. As described above, we use the access point firmware provided by the OpenWRT project. By using this firmware, we can obtain several performance metrics in the access point described below.

By use of the OpenWRT firmware, we can configure the queue management schemes used in the access point. It supports the following schemes.

- *FIFO*: A scheme to use one queue to store all frames being sent by the access point.

ISBN: 978-1-61208-503-6

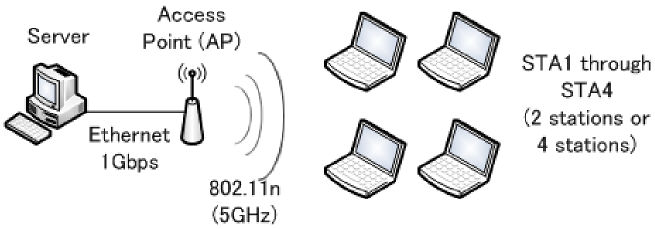


Figure 1. Configuration of experiment.

TABLE I. SPECIFICATIONS OF STAs AND ACCESS POINT (AP)

STA	Manufacturer/Model	DELL Insilon 14
	Operating system	Ubuntu 14.04LTS (kernel 3.13)
AP	Manufacturer/Model	BUFFALO AirStation WZR-HP-AG300H
	Firmware	OpenWRT (BarrierBraker, r444, selfbuild)
	WLAN chip	Atheros AR7161
	WLAN driver	ath9k

- *CoDel* [7]: An active queue management scheme designed to resolve the Bufferbloat problem [8]. It uses packet-sojourn time in a queue as a control parameter, and drops one packet among those staying in the queue too long.
- *Stochastic Fare Queueing* (*SFQ*): A scheme to provide a separate queue for packets of an individual flow.
- *FQ_CoDel*: A scheme which combines SFQ and CoDel. In OpenWRT, FQ_CoDel is the default queue management scheme.

In the experiment, we used all those queueing management schemes for the performance evaluation.

The access point uses two streams in the spatial division multiplexing with each channel using 60 MHz bandwidth, and, as a result, the data rate ranges from 6.5 Mbps to 300 Mbps.

In the experiment, data is transferred from the server to two or four stations through the access point. The server uses *iperf* tool [9] to generate TCP data segments. As for TCP parameter settings, we used the native ones in the Linux operating system. Specifically, the TCP version is CUBIC TCP.

During the data transfer, the following performance metrics data are collected for the detailed analysis for the communication;

- MAC level data rate (an average during one second, collected at the access point for individual A-MPDUs from the ath9k device driver [10]),
- the number of MPDUs per A-MPDU (an average during one second, collected at the access point for individual A-MPDUs from the device driver),
- TCP throughput (an average during one second, measured at the server by use of *tcpdump*),
- cwnd (an average during one second, measured at the server for every data segment sent by use of *tcpprobe* [11]), and
- TCP level RTT (an average during one second, measured at the server for every ACK segment received).

From measured cwnd and RTT values, we calculate the estimated TCP load by the following equation.

$$Estimated\ load\ (Mbps) = \frac{cwnd*1{,}500*8}{RTT*1{,}000{,}000} \qquad (1)$$

The experiment is conducted in a building constructed with reinforced concrete. Fig. 2 shows the layout inside the building and the positions of network equipment. The thick black line represents the exterior wall of the building and the thin black line represents the interior wall, which is made from wood.

In the case of two station experiment, the black circles named "AP" and "STA1" correspond to the positions of the access point and the near station, STA1, respectively. These are fixed throughout the experiment. The black circles named "Position0" through "Position7" represent the positions of the far station, STA2. It is located in one of these eight positons in the experiment.

In four station experiment, three stations, STA1 through STA3, are located at position "STA1" and the other station, STA4, is located at one of positions from "Position0" to "Position7."

III. RESULTS FOR TWO STATION EXPERIMENT

A. Experimental Scheme

In the two station experiment, we measured the performance of TCP data transfer from the server to the stations, by changing the position of STA2 and the queue management scheme in the access point. For each STA2 position and queue scheme, we executed three experiment runs, each of which is 120 second TCP data transfer.

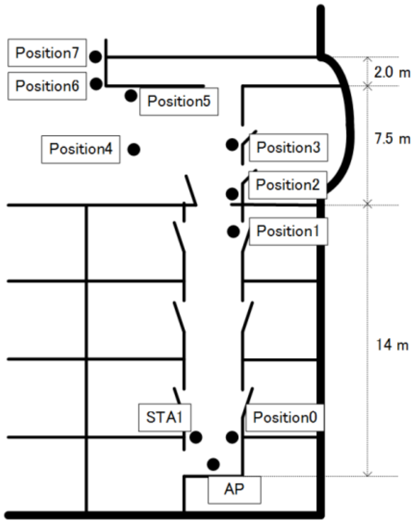


Figure 2. Layout inside building and position of equipment.

B. *Overall Results*

Fig. 3 shows the relationship between the position of STA2 (“PS” in the figure means “Position”) and the average of MAC level data rate of STA1 and STA2. STA1 located near the access point keeps high data rate around 250 Mbps. On the contrary, the average data rate of STA2 decreases along with its location being far away from the access point. More specifically, the data rate of STA2 takes a similar value for Position3 and Position4, and Position6 and Position7. Fig. 3 is the result when the FIFO queue management scheme is used at the access point. The cases when the other schemes are used showed similar results. In the rest of this paper, the position of STA2 (far located station) is represented its average data rate.

Fig. 4 shows the relationship between the STA2 average data rate and the average TCP throughput (average values throughout three experimental runs). In this graph, solid lines indicate the results of STA1 and dashed lines indicate those of STA2, and the color of lines corresponds to the individual queue management scheme. The TCP throughput of not only STA2 but also STA1 decreases as the position of STA2 becomes far from the access point. There was no difference among the queue management schemes in the access point.

Fig. 5 (a) shows the average cwnd versus the STA2 average data rate. In this case, the results largely depend on the queue management schemes. In FIFO, the average cwnd is large and varied from 1 to 900 packets. In SFQ, the queue length for an individual flow is limited to 127 packets, and this in turn limits the cwnd. CoDel and FQ_CoDel drop packets which stay in the queue for a long time, and so the cwnd is suppressed. In all queue schemes, the average cwnd is small when STA2 is located at Position6 and Position7. In this situation, there seems to be a lot of packet losses in both STA1 and STA2 TCP flows.

Fig. 5 (b) shows the average TCP level RTT versus the STA2 average data rate. Here, the results also depend on the queue management scheme. Especially, FIFO has a large RTT compared to the other schemes. In FIFO, both cwnd and RTT are larger than the others, but, since both of them are larger in the similar magnitude, the throughput is also similar with the others.

We consider that the overall results are not enough to explain the results for TCP flows. So, we explain the detailed analysis below.

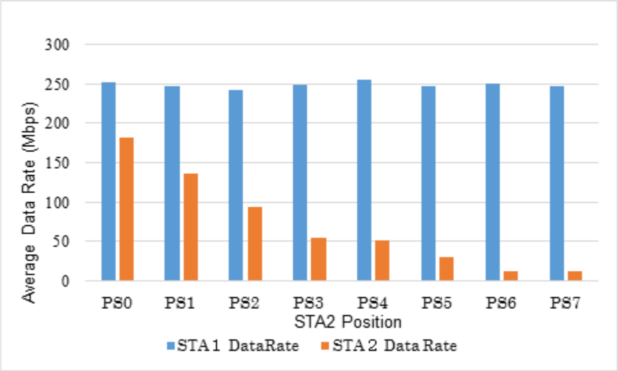


Figure 3. Average MAC level data rate vs. STA2 position (FIFO).

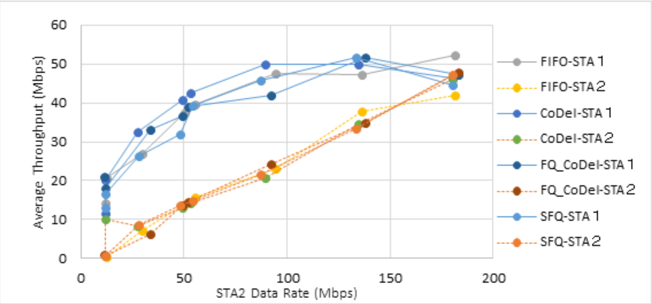
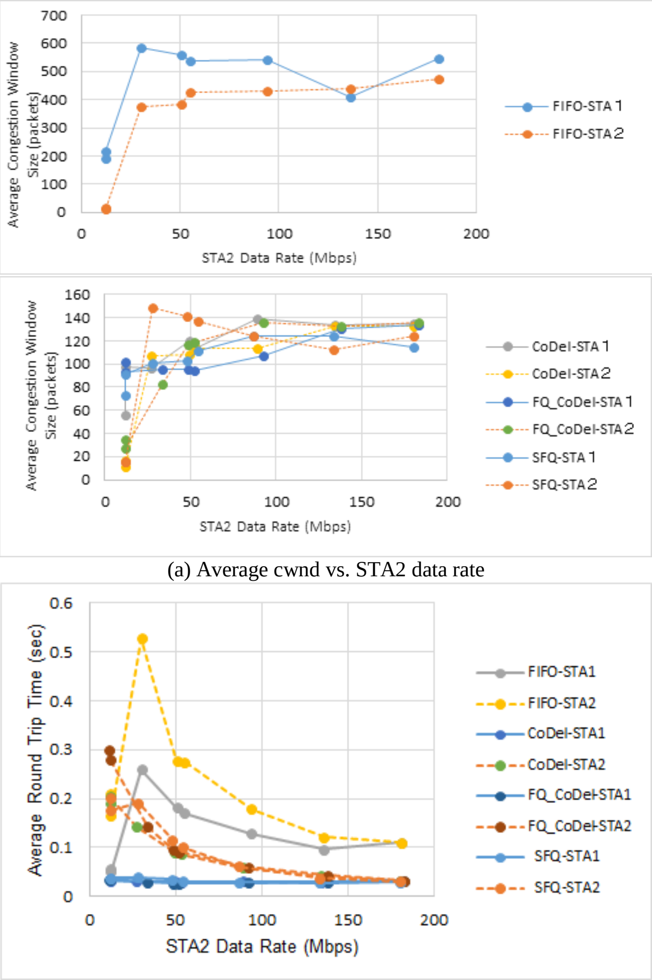


Figure 4. Average TCP throughput vs.STA2 data rate.



(a) Average cwnd vs. STA2 data rate

(b) Average RTT vs. STA2 data rate

Figure 5. Average cwnd and RTT.

C. *Detailed Results*

Figs. 6, 7 and 8 show the time variation of TCP throughput of STA1 and STA2 when STA2 is located at Position0, Position 4 and Position7, respectively. Those results are obtained by use of FIFO at the access point.

When STA2 is located at Position0, the TCP throughput of STA1 and STA2 varies around 50 Mbps. Throughout 120 sec. data transfer, two stations provide high TCP throughput. In the time frames from 50 sec. to 70 sec. and after 90 sec., the

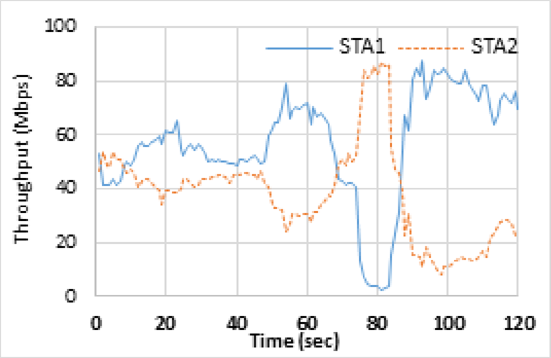


Figure 6. Time variation of TCP throughput when STA2 is located at Position0.

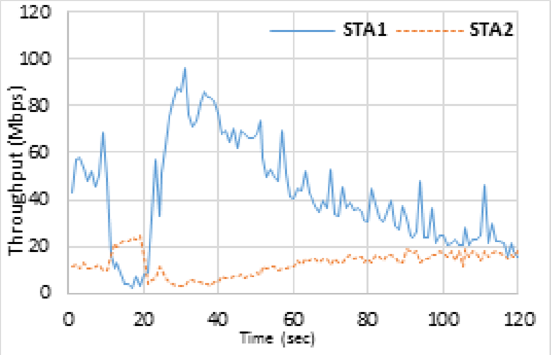


Figure 7. Time variation of TCP throughput when STA2 is located at Position4.

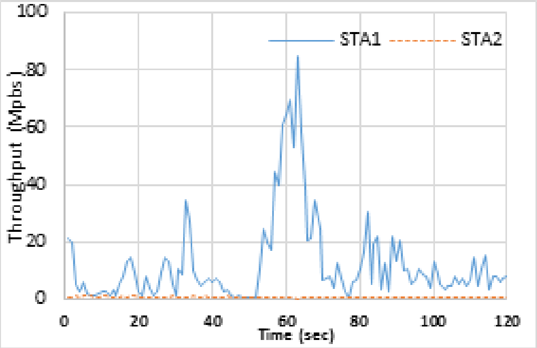


Figure 8. Time variation of TCP throughput when STA2 is located at Position7.

TCP throughput of STA1 is higher, and between 70 sec. and 90 sec., STA2 provides higher throughput. It can be said that two stations conflict for the WLAN channel rather fairly.

When STA2 is located at Position4, the TCP throughput of STA1 is 40 Mbps through 60 Mbps in the beginning, but it falls down in 10 sec. through 20 sec. It grows to 80 Mbps again, but after that, it decreases gradually to the value similar to STA2. In the case of STA2, the TCP throughput is less than 20 Mbps.

When STA2 is located at Position7, the TCP throughput of STA2 is very low and around 1 Mbps. The throughput of STA1 is lower than 20 Mbps in most of time, but is as high as 80 Mbps around 60 sec.

Throughout those experimental runs, the MAC level data rate is almost constant both for STA1 and STA2. On the other hand, the TCP throughput, especially that of the near station, fluctuates largely. When STA2 is located at Position7, the throughput of STA1 is lower than the other cases, but it has a time frame when the throughput is high.

In order to examine the reason of this fluctuation, Figs. 9 and 10 show the time variation of cwnd and RTT, when STA2 is located at Position4 and Position7, respectively. In Fig. 8, the cwnd of STA1 decreases sharply at 10 sec., goes to 1000 packets and then decreases gradually. The cwnd of STA2 is around 200 packets until 20 sec., but it decreases sharply and then it is going up gradually. These results show that the variation of cwnd is closely related with the variation of TCP throughput. On the other hand, the time variation of RTT has a frequent fluctuation but the value is smaller than 300 m sec. in most of time. Fig. 10 gives similar results. The graph of the time variation of cwnd is similar with that of the TCP throughput. The RTT values are also less than 300 m sec. in most of time. From those results, it can be decided the TCP throughput of STA1 is determined by the time variation of cwnd, which is decreased by packet losses.

In the previous paper [5], we showed that the performance anomaly occurs in UDP flows when the UDP traffic load to far located station is larger than its MAC level data rate. So, we calculated the estimated TCP load from equation (1) using the results given in Figs. 9 and 10. Figs. 11 and 12 show the time variation of the estimated TCP load and the data rate in STA2 when it is located at Position4 and Position7, respectively. Those results indicate that the estimated load is much smaller than the MAC level data rate. That is, the traffic

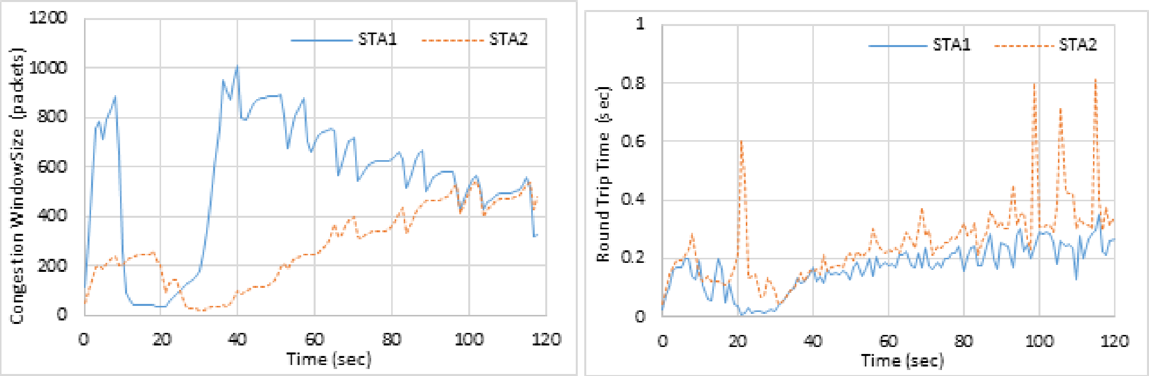


Figure 9. Time variation of cwnd and RTT when STA2 is located at Position4.

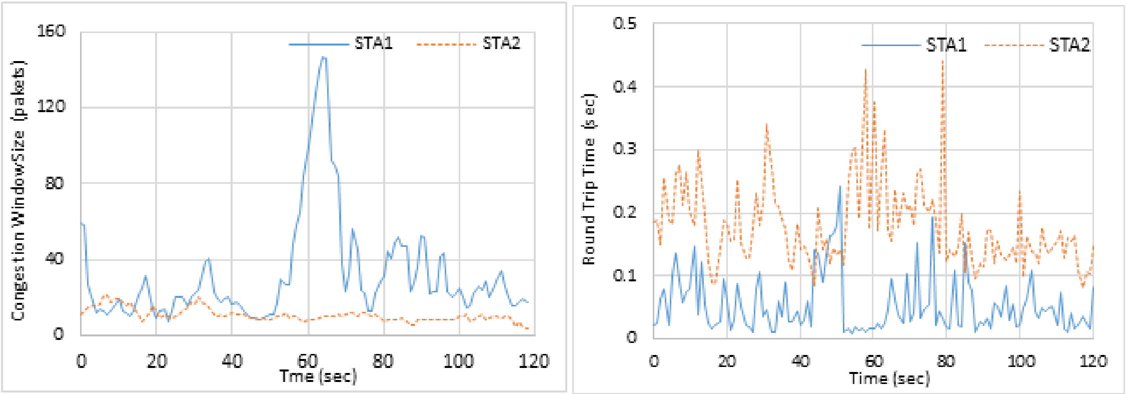


Figure 10. Time variation of cwnd and RTT when STA2 is located at Position7.

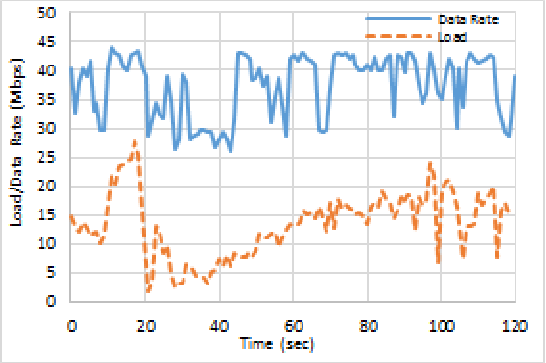


Figure 11. Time variation of estimated TCP load and data rate in STA2 when it is located at Position4.

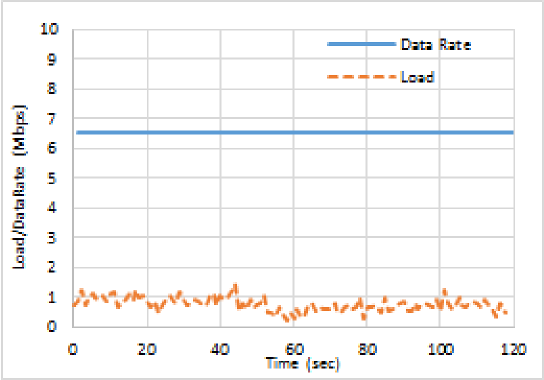


Figure 12. Time variation of estimated TCP load and data rate in STA2 when it is located at Position7.

load to STA2 is smaller than the transmission speed for STA2. Therefore, it can be concluded that, in the case of TCP download data transfer, the performance anomaly does not occur in a strict sense. That is, the throughput of a near station is not reduced to the similar value of a far located station. The reason the throughput is degraded is that the cwnd value in a near station is decreased due to packet losses.

So far, we used the FIFO queue management scheme at the access point. We also tried the other queue management schemes; CoDel, SFQ and FQ_CoDel. Although the cwnd values in STA1 and STA2 are smaller than the case in FIFO, we had a similar trend that the estimated TCP load to STA2 is much smaller than its MAC level data rate.

IV. Results for Four Station Experiment

Next, we conducted a similar experiment using four stations. As described in Section 2, we used the configuration where three stations, STA1 through STA3, are located at STA1's position so far and the other station, STA4, is located at one of positions "Position0" through "Position7." Similarly with the two station experiment, we use the average data rate of STA4 to represent its position.

Fig. 13 shows the relationship between the position of STA4 and the average of MAC level data rate of STA1 through STA4. The average data rate of STA4 decreases along with its location being far away from the access point. On the other hand, the average data rate of STA1, STA2 and STA3 located near to the access point is rather high, such as 250 Mbps or higher, except that STA2 sometimes takes 150 Mbps or 200 Mbps average data rate. This is the result when the FIFO queue management scheme is used. The cases when the other schemes are used showed similar results. Similarly with the two station experiment, we use the average data rate of STA4 to represent its position.

Fig. 14 (a) shows the relationship between the STA4 average data rate and the average TCP throughput of all stations. In this experiment, the average TCP throughput of near stations did not decrease so much as the STA4 average data rate goes down. This is in contrast with the result of two station experiment. The average throughput of far station (STA4) decreases much more than the others along with it located far from the access point. This result clearly shows that the performance anomaly does not occur in the case of three near stations and one far station.

Fig. 14 (b) shows the average cwnd of all stations versus the STA4 average data rate. In the four station experiment, the cwnd values are similar among all the stations including STA4, although cwnd of STA4 is slightly reduced when its average data rate is smaller than 50 Mbps. The values are between 200 and 350 packets, which are smaller than the two station experiment, and this means that there are more packet losses and more cwnd drops than the two station case.

Fig. 14 (c) shows the average TCP level RTT of all stations versus the STA4 average data rate. The average RTT for STA1 through STA3 does not change so much even if the STA4 average data rate becomes small. On the other hand,

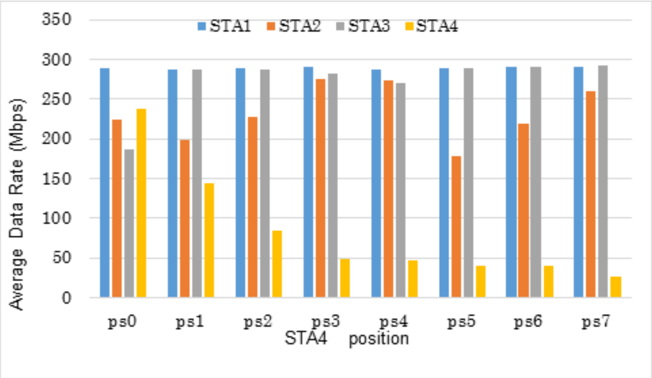
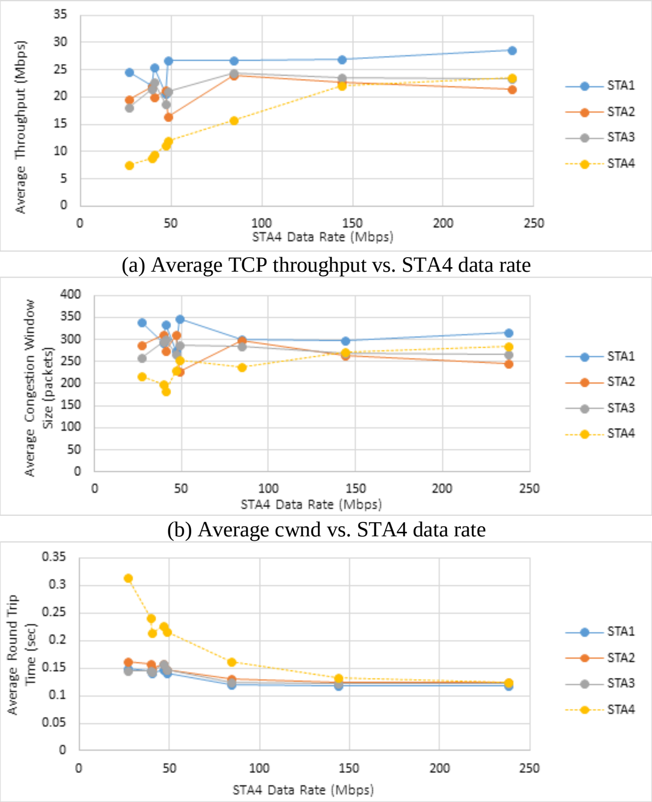


Figure 13. Average MAC level data rate vs. STA4 position (FIFO).



(a) Average TCP throughput vs. STA4 data rate

(b) Average cwnd vs. STA4 data rate

(c) Average TCP level RTT vs. STA4 data rate

Figure 14. Average TCP throughput, cwnd and RTT (FIFO).

that for STA4 increases when its average data rate becomes small. This increase of RTT is considered as the reason of the average TCP throughput of STA4 being decreased in the small STA4 data rate.

In summary, in the situation where three near stations and one far station share an access point, the TCP download data transfer in the near stations is not influenced by that of the far station. The impact of far station is smaller than the situation where one near station and one far station exist. This is different from the results stated in [4].

V. CONCLUSIONS

This paper discussed the performance anomaly of TCP flows providing download data transfer over IEEE 802.11n WLAN. We conducted two station and four station experiments, where one of the stations is located far from the access point. We used a commercially available access point using four queuing management schemes in it. We measured several performance metrics including the MAC level data rate, the number of MPDUs aggregated in an A-MPDU, the TCP throughput, the congestion window size, and the TCP level round trip time.

In the two station experiment, the TCP throughput of the near station is degraded along with the distance between the far station and the access point increasing. However, we conclude that this is not the performance anomaly in a strict sense. The reason is that the estimated TCP load to the far station is much lower than its MAC level data rate. Instead, we conclude that the throughput degradation comes from the decrease of the congestion window size caused by packet losses.

In the case of four station experiment, the degradation of the TCP throughput of near stations was smaller than the two station experiment. This means that the data transfer to the far station gives only a small impact to the near stations. This will be also the evidence that the performance anomaly does not occur in the TCP flows.

As for the queue management scheme, there was only a little influence in terms of TCP throughput. We also conducted an experiment using the native firmware of the access point and obtained the similar results.

REFERENCES

[1] IEEE Standard for Information technology: Local and metropolitan area networks Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2012.

[2] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, “Performance Anomaly of 802.11b,” Proc. INFOCOM 2003, vol.2, pp.836-843, Mar. 2003.

[3] M. Abusubaih, “On Performance Anomaly in 802.11 Wireless LANs: Problem and Solution Approaches,” Proc. Next Generation Mobile Applications, Services and Technologies (NGMSAT) 2010, pp.208-212, Jul. 2010.

[4] O. Abu-Sharkh and M. Abdelhadi, “The impact of multi-rate operation on A-MSDU, A-MPDU and block acknowledgment in greenfield IEEE802.11n wireless LANs,” Proc. Wireless Advanced (WiAd) 2011, pp. 116-121, Jun. 2011.

[5] Yoshiki Hashimoto, Masataka Nomoto, Celimuge Wu, Satoshi Ohzahata, and Toshihiko Kato, “Experimental Analysis on Performance Anomaly for Download Data Transfer at IEEE 802.11n Wireless LAN,” Proc. International Conference on Networks (ICN) 2016, pp.22-27, Feb. 2016.

[6] “Open Wrt Wireless Freedom,” https://www.openwrt.org/, retrieved: Feb. 2016.

[7] K. Nichols and V. Jacobson, “Controlling Queue Delay,” ACM Queue, Networks, vol.10, no.5, pp. 1-15, May 2012.

[8] J. Gettys and K. Nichols, “Bufferbloat: Dark Buffers in the Internet,” ACM Queue, Virtualization, vol. 9, no.11, pp. 1-15, Nov. 2011.

[9] iperf, http://iperf.sourceforge.net/, retrieved: Feb. 2016.

[10] ath9k Linux Wireless, http://wireless.kernel.org/en/users/Drivers/ath9k, retrieved: Feb. 2016.

[11] Linux foundation: tcpprobe, http://www.linuxfoundation.org /collaborate/workgroups/networking/ tcpprobe, retrieved: Feb. 2016.

Extent-Based Allocation Scheme for Hybrid Storage Solutions

Jaechun No
College of Electronics and Information Engineering
Sejong University
Seoul, Korea
email:jano@sejong.ac.kr

Sung-soon Park
Dept. of Computer Science and Engineering
Anyang University and Gluesys Co. LTD
Anyang, Korea
email:sspark@gluesys.com

***Abstract*—We present an extent-based allocation scheme for hybrid storage solutions, called MatBall (Matrix and extent-based allocation), whose objective is to increase space utilization of SSD (Solid State Device) partition in the hybrid file system by reducing fragmentation overhead. In MatBall, to consume the remaining spaces as much as possible posterior to file allocations, I/O units (extents) of the hybrid file system are recursively partitioned into segments in the subsequent level and further file allocations are performed in units of the partitioned segments. Since MatBall defines easy-to-compute segment sizes and block positions in I/O units, allocating more files in the remaining spaces can be performed with a little overhead. The performance measurement with IOzone shows that the hybrid file system using MatBall enables to produce higher bandwidth over ext2 installed on HDD (Hard Disk Drive) and SSD.**

Keywords-extent partitioning; matrix-based allocation; file mapping; fragmentation overhead.

I. INTRODUCTION

SSD [1]-[4] technology has dramatically improved over decades to become an essential component in storage solutions. Due to the fact that SSD does not need the mechanical overhead, such as seek time, to locate the desire data, it has drawn great attention from IT markets that seek for improved I/O performance. The key obstacle to the widening SSD adoption to large-scale storage subsystems is its high cost per capacity, compared to that of HDD. Even though the cost of flash memory becomes decrease, the price of SSD is still much higher and such a high cost/capacity ratio makes it less desirable to construct large-scale storage subsystems solely composed of SSD devices.

There are several ways of utilizing SSD advantages to boost I/O performance [5]-[8][12]. The first one is to implement SSD-related I/O optimizations in the file system level. For example, Josephson et al. [6] uses fusion-io ioDrive to provide the virtualization flash storage layer that acts as the traditional block device driver with FTL (Flash Translation Layer). Also, Lee et al. [7] proposed a new filesystem metadata platform that can reduce SSD-specific semiconductor overheads.

Although those file systems have successfully integrated SSDs to improve I/O performance, adapting a new file system to the existing storage solutions is not easy because it should go through the long, pains-taking process to prove the durable data consistency and reliability.

An alternative is to use hybrid storage subsystems, which are managed by the hybrid file system or SSD-specific cache [9-11]. In such methods, a small portion of SSD partition is combined with a much larger HDD storage capacity in a cost-effective way, while making use of the strengths of both devices. Since only a small-size of file system address space is provided by SSD partition, increasing space utilization for SSD partition has a critical impact in improving I/O performance.

In this paper, we propose an extent-based file allocation approach, called MatBall. The primary objective of MatBall is to increase the usage of the costly SSD storage resources as much as possible in the hybrid file system, by reusing the remaining spaces of I/O units and thus by decreasing fragmentation overhead. In the hybrid file system where the entire address spaces are constructed on both SSD and HDD partitions, MatBall can contribute to maximize the space usage of SSD partition by taking responsibility of allocating files in SSD partition.

The rest of paper is organized as follows: In Section II, we present the implementation details of MatBall. The performance results of MatBall integrated with the hybrid file system are shown in Section III. In Section IV, we conclude our paper.

II. IMPLEMENTATION DETAILS

We present the segment partitioning and file mapping.

A. System Model

In MatBall, I/O unit is an extent. However, an extent is composed of a group of segments and the allocation on the extent is performed in units of segments to reduce extent fragmentation.

Definition 1 (extent structure) An extent of size s in blocks is a finite set of segments such that: 1) there are $\log_2 s+1$ number of segments at the top level (level 0), with each being indexed from H to $(\log_2 s)-1$; 2) segment j at level L whose size is larger than or equal to a threshold λ is partitioned into $j+1$ segments at the subsequent level $L+1$ and their indices are ranged from H to $j-1$. The segment partitioning is continued until the size of every segment is smaller than λ.

The segment with index H is called the head segment.

The segment *j* of level *L* being partitioned from segment *i* of level *L*-1 is the child and denoted as *seg*[*i*,*k*]. On the other hand, segment *t* of level 0 is denoted as *seg*[*,*t*].

The starting block position of segment *j* of level *L* is *pos*(*seg*[*i*,*j*])=*pos*(*seg*[*i*,*H*])+2^j where *j*>*H*. If *j*=*H*, then *pos*(*seg*[*i*,*j*]) is the same to the starting block position of segment *i*. The size of segment *j* is 2^j, except for the head segment that is composed of a single block.

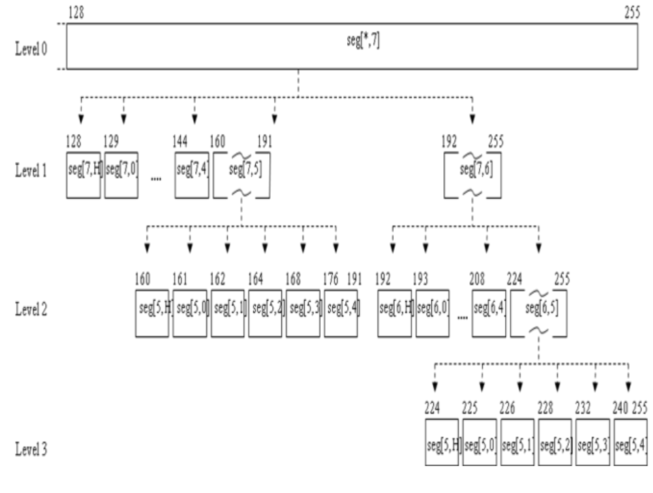


Figure 1. An example of segment partitioning.

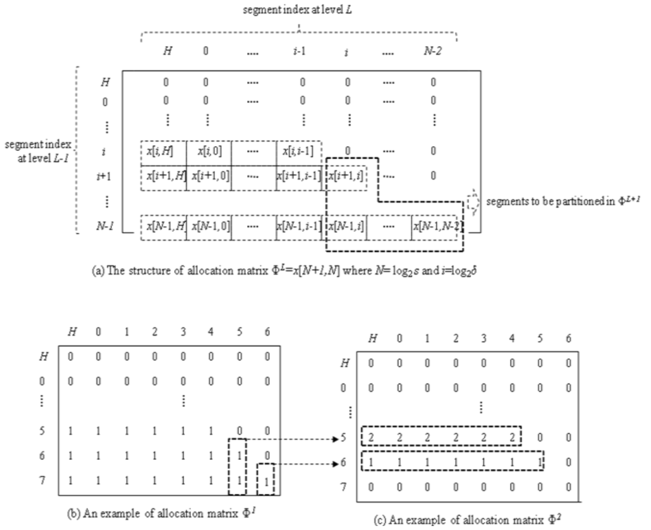
Figure 1 illustrates an example of segment partitioning with λ =32. An extent with 256 blocks is partitioned into nine segments from *seg*[*,*H*] to *seg*[*,7] at the top level. Since the threshold is set to 32, the segments whose size is larger than or equal to 32 in blocks are partitioned at the subsequent level until each segment has the size of less than 32 blocks. In Figure 1, *seg*[*,7] is split into eight segments at level one and segments *seg*[7,5] and *seg*[7,6] are in turn partitioned at level two due to their sizes. The maximum segment index is decreased by one, in case the segment partitioning takes place at the subsequent level.

B. Allocation Matrix

The segment partitioning of MatBall takes place using the allocation matrix, which is organized at each level.

Definition 2 (Allocation matrix) An allocation matrix $\varPhi^L = x[N+1, N]$ where *N*=log₂*s* is an abstraction of the segment partitioning at level *L*>0 such that: 1) each row *i* $(H \le i < \log_2 s)$ shows the segment index of the parent at level *L*-1; 2) column *j* $(H \le j < (\log_2 s) - 1)$ shows the index of segment at level *L* that is partitioned from parent *i*.

Figure 2(a) shows the allocation matrix $\varPhi^L$ where $N = \log_2 s$ and $i = \log_2 \lambda$. There are two aspects in the allocation matrix. First of all, the segments from *seg*[*i*+1,*i*] to *seg*[*N*-1,*N*-2] should be partitioned at level *L*+1 since their size is larger than equal to λ. Second, some of them can have the same indices at the subsequent level. For example, segments from *seg*[*i*+1,*i*] to *seg*[*N*-1,*i*] contain *seg*[*i*,*H*] to *seg*[*i*,*i*-1] at level *L*+1. In $\varPhi^L$, *x*[*i*,*j*] is the number of segments with index *j* at level *L* that are partitioned from the segments with index *i* at level *L*-1. If *x*[*i*,*j*]=0 for row *i*, then no segment partitioning takes place at level *L*.


segment index at level L
segment index at level L-1
segments to be partitioned in Φ^{L+1}

$$\begin{array}{c|ccccccc} & H & 0 & \cdots & i\text{-}1 & i & \cdots & N\text{-}2 \\ \hline H & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ i & x[i,H] & x[i,0] & \cdots & x[i,i\text{-}1] & 0 & \cdots & 0 \\ i\text{+}1 & x[i\text{+}1,H] & x[i\text{+}1,0] & \cdots & x[i\text{+}1,i\text{-}1] & x[i\text{+}1,i] & \cdots & 0 \\ \vdots & & & & & & & \\ N\text{-}1 & x[N\text{-}1,H] & x[N\text{-}1,0] & \cdots & x[N\text{-}1,i\text{-}1] & x[N\text{-}1,i] & \cdots & x[N\text{-}1,N\text{-}2] \end{array}$$

(a) The structure of allocation matrix Φ^L=*x*[*N*+*1*,*N*] where *N*= log₂*s* and *i*=log₂*δ*

$$\begin{array}{c|cccccccc} & H & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline H & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & & & & \vdots & & & & \\ 5 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 7 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

(b) An example of allocation matrix Φ^1

$$\begin{array}{c|cccccccc} & H & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline H & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & & & & \vdots & & & & \\ 5 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 \\ 6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

(c) An example of allocation matrix Φ^2

Figure 2. An example of allocation matrix.

Figure 2(b) and (c) show the allocation matrix $\varPhi^1$ and $\varPhi^2$ for an extent of size 256 blocks. The allocation matrix consists of nine rows and eight columns. The rows of $\varPhi^1$ denote the segments of the top level from *seg*[*,*H*] to *seg*[*,7]. Among them, *seg*[*,5] to *seg*[*,7] are partitioned at level one because their sizes are at least λ. Also, the children of *seg*[6,5] and *seg*[7,5] contain *seg*[5,H] to *seg*[5,4] at level two and thus *x*[5,*H*] to *x*[5,4] of $\varPhi^2$ are marked as two. On the other hand, *x*[6,*H*] to *x*[6,5] are set to one because only *seg*[7,6] of $\varPhi^1$ is involved in the segment partitioning. Since *x*[6,5]>0 in $\varPhi^2$, one more partitioning would take place at $\varPhi^3$.

Theorem 1. Given an extent of size s in blocks, the number of allocation matrices for the segment partitioning is $\log_2(s/\lambda)$. Also, using $\varPhi^L$, the maximum number of segments available at level *L* is:

$$\sum_{i=a}^{b}(x[i,H] + \sum_{k=0}^{i-1} x[i,k]),\ a = \log_2 \lambda \text{ and } b = (\log_2 s) - 1$$

Proof. In MatBall, the segments with indices between $\log_2 \lambda$ and (log₂s)-1 are partitioned at each level. Therefore, the number of levels for the segment partitioning is $\log_2 s - \log_2 \lambda$, resulting in $\log_2(s/\lambda)$ allocation matrices to be created. In $\varPhi^L$, the number of segments to be generated from segment *i* of level *L*-1 is $x[i,H]+\sum_{j=0}^{i-1}x[i,j]$. Also, the segments that are subject to the segment partitioning at level *L*-1 are from $\log_2\lambda$ to ($\log_2$s)-1. Thus, the number of segments available at level *L* is $\sum_{i=\log_2\lambda}^{(\log_2 s)-1}(x[i,H]+\sum_{j=0}^{i-1}x[i,j])$

In Figure 2(b), *seg*[*,5] of the top level is partitioned to {*seg*[5,*H*], *seg*[5,0], *seg*[5,1], *seg*[5,2], *seg*[5,3],*seg*[5,4]}. Since only a single child with such an index is available at level one, the associated elements in Φ^1 is set to one. The same procedure is applied to *seg*[*,6] and *seg*[*,7]. As a result, the total number of segments available at level one is $\sum_{i=5}^{7}(x[i,H]+\sum_{j=0}^{i-1}x[i,j])=21.$

C. Segment Mapping

In this Section, we describe a hierarchical, fine-grained way of mapping data to segments consisting of extents. The segment mapping of MatBall was designed to collect data in an extent as many as possible, to improve the space utilization of extents. Also, the starting position of the segment mapping can be easily calculated by referencing the hierarchical structure of extents.

Definition 3 (Segment mapping) Given $\Phi^L = x[N+1,N]$, assume that a sequence of the segment partitioning for row *i* (*i*>*H*) is given by

$$seg[*,a]\rightarrow seg[a,b]\rightarrow\cdots\xrightarrow{L-1}seg[o,i]\xrightarrow{L}seg[i,j]$$

Then the starting block position of segment *j* at *L* is $pos(seg[i,j])=2^a+2^b+\cdots+2^i+2^j$.

Since the block position of the head segment is ze ro, *pos*(*seg*[*,*a*]) is 2^a. Furthermore, child *b*>*H* of level one has the size of 2^b in blocks, thus *pos*(*seg*[*a*,*b*])=2^a+2^b. As a result, segment *j* generated from *i* has the starting block position of $2^a+2^b+\cdots+2^i+2^j$. Likewise, for the children of segment *j*, *pos*(*seg*[*j*,*H*]) = *pos*(seg[*i*,*j*]) and *pos*(seg[*j*,*k*])=*pos*(*seg*[*i*,*j*])+2^k where *k*>*H*.

For example, in Figure 1, suppose that a file has been allocated to an extent from block position zero to 165. First of all, the ending block position 165 falls into segment seven. Due to its size larger than λ, the partitioning at the level one takes place:

$$\text{I}\ )\xrightarrow{level0}2^7\le 165<2^8,$$
$$size(seg[*,7])=2^7>\lambda,\ pos(seg[*,7])=2^7$$

The child segment five being partitioned from segment seven of the top level contains the block position 165 and the starting position of child five is calculated by adding its size to its parent starting position:

$$\text{II})\xrightarrow{levle1}2^5\le 165-pos(seg[*,7]<2^6,$$
$$size(seg[7,5])=2^5>\lambda,\ pos(seg[7,5])=pos(seg[*,7])+2^5$$

Since the size of child five is still the same to λ, one more partitioning at level two takes place, resulting in mapping block potion 165 to segment two at level two. The starting position of segment two is obtained by applying the same way we did in the upper level:

$$\text{III})\xrightarrow{levle2}2^2\le 165-pos(seg[7,5]<2^3,$$
$$size(seg[5,2])=2^2<\lambda,\ pos(seg[5,2])=pos(seg[7,5])+2^2$$

As a result, the next file allocation in the same extent takes place from segment three of level two that begins at block position 168:

pos(*seg*[5,3]) = *pos*(*seg*[*,7])+*pos*(*seg*[7,5])+2^3=168.

```
Algorithm: MAP (input:w, output:level, index, next)

1.  compute j such that $2^j \le w < 2^{j+1}$; level=0;
2.  if $j < \log_2\lambda$
3.      index=k+1; next=pos(seg[*,j+1]);
4.      return
5.  end if
6.  pos = pos(seg[*,j]);
7.  while $j \ge \log_2\lambda$ do
8.      level ++;
9.      find k such that $2^k \le w - pos < 2^{k+1}$;
10.     if $k < \log_2\lambda$
11.         index=k+1; next=pos(seg[j,k+1]);
12.         return
13.     end if
14.     pos = pos(seg[j,k]);
15.     j= k;
16. end while
```

Figure 3. File allocation algorithm on extents.

Figure 3 shows the steps involved in finding the segment where the next file allocation begins on the extent. Let *w* be the ending block position of the last file allocation. The output of the algorithm is *level*, *index* and block position *next* where the next file allocation starts. In the algorithm, step 2 to 5 executes file allocation without the segment partitioning and takes O(1). Step 7 to 16 shows the segment partitioning taking place when the size of segment mapped to *w* is larger than or equal to λ. Since the maximum number of the segment partitioning is $\log_2(s/\lambda)$, the time complexity of the algorithm is O(log$_2$*s*). In MatBall, only the extents containing at least λ free blocks are reused for space utilization.

Theorem 2. Given an extent *E* of size *s* in blocks, let $\lambda = 2^n (n \geq 1)$ and *L* be the number of levels of the segment partitioning. Then, with $\delta = 2^m (m \geq 1)$ such that $\delta < \lambda,$ the levels needed for partitioning is $L + \log_2(\lambda/\delta).$ Also, let *w* ($s - w \geq \lambda + 1$) be the ending block position of the last file allocation of *E* and *p* and *q* be the hole sizes with λ and $\delta,$ respectively. Then $p \geq q.$

Proof. With δ and $\lambda,$ since the number of levels for the segment partitioning is $\log_2(s/\delta)$ and $\log_2(s/\lambda),$ the level difference between two thresholds is $\log_2(\lambda/\delta).$ Therefore, for $\delta(<\lambda),$ it needs $L + \log_2(\lambda/\delta)$ partitioning levels at maximum. Assume that *w* is mapped to segment *i* at level *X* on *E*. Let *o* be the parent of *i* at level ***X***-1.

case $(i < \log_2 \delta):$ no segment partitioning takes place on *i* with two thresholds. In this case, the next allocation occurs at *pos*(*seg*[*o*,*i*+1]). As a result, *p*=*q*= *pos*(*seg*[*o*,*i*+1])-(*w*+1).

case $(\log_2 \delta \leq i < \log_2 \lambda):$ *i* is not partitioned with λ and thus *p* = *pos*(*seg*[*o*,*i*+1])-(*w*+1). On the other hand, with $\delta,$ segment *i* is partitioned into the lower level *X*+1. Let *k* be the segment of *X*+1 where *w* is mapped. Then, the next file allocation on *E* begins at segment *k*+1. Since *pos*(*seg*[*i*,*k*+1]) < *pos*(*seg*[*o*,*i*+1]), *q* = *pos*(*seg*[*i*,*k*+1])-(*w*+1) < *p*.

case $(i \geq \log_2 \lambda):$ segment *i* with δ is more partitioned than with λ due to $\delta < \lambda.$ Also, the more a segment is partitioned, the smaller the hole size is between two consecutive file allocations on *E*. Therefore, *q*<*p*.

Theorem 2 implies that there is a tradeoff between partitioning overhead and space utilization, regarding to the threshold value. With the small threshold value, the hole size between two consecutive file allocations on an extent becomes small. However, it might need more partitioning steps than with a larger value. Our objective in using the allocation matrix is to choose the appropriate partitioning threshold to reduce extent fragmentation while minimizing the partitioning overhead.

III. PERFORMANCE EVALUATION

We present the performance measurement of MatBall.

A. Experimental Platform

We integrated MatBall with the hybrid file system. In the hybrid file system, the entire address space is constructed by combining a small portion of SSD partition with HDD partition. The file allocation of SSD partition is executed by performing MatBall, therefore the files are allocated per extent composed of a group of segments.

When the hybrid file system is mounted, the clean extents that are not used for file allocations yet and the allocation matrices are organized in memory. Also, I/O request is simultaneously performed on both partitions. When either of partitions completes I/O, control returns user.

Table 1 illustrates the number of allocation matrices and partitioning description for each extent size and threshold value $\lambda.$ We evaluated MatBall with IOzone while comparing it with ext2 installed on HDD and SSD.

TABLE Ⅰ SEGMENT PARTITIONING BASED ON EXTENT SIZE

extent size	λ	# of allocation matrices	partitioning description
64	16	2	$\xrightarrow{level0} \{seg[*,H], seg[*,0], \cdots, seg[*,5]\}$ *seg*[*,4] and *seg*[*,5] are involved in the subsequent segment partitioning.
	32	1	$\xrightarrow{level0} \{seg[*,H], seg[*,0], \cdots, seg[*,5]\}$ only *seg*[*,5] is involved in the subsequent segment partitioning.
256	16	4	$\xrightarrow{level0} \{seg[*,H], seg[*,0], \cdots, seg[*,7]\}$ *seg*[*,4] to *seg*[*,7] are involved in the subsequent segment partitioning.
	32	3	$\xrightarrow{level0} \{seg[*,H], seg[*,0], \cdots, seg[*,7]\}$ *seg*[*,5] to *seg*[*,7] are involved in the subsequent segment partitioning.

The performance measurements are executed on a PC with AMD Athlon dual-core processor and 1GB of memory. The HDD partition is equipped with a 320GB of Seagate 7200 RPM disk and SSD partition uses fusion-io SSD ioDrive. We used CentOS release 6.2 with a 2.6.18 kernel. The hybrid file system integrated with MatBall uses database built on SSD partition.

B. IOzone Experiment

We evaluated MatBall using IOzone, while varying file sizes from 64KB to 256MB. We executed *./iozone –azi –e –g* 256M *–q* 8K to use 8KB of I/O record size. We used *fsync*() in every I/O operations to reduce the effect of memory cache. Also, for each I/O operation, we changed the threshold value for the segment partitioning from 16 to 32, to observe the partitioning overhead.

Figure 4 and 5 show the write performance of MatBall, while comparing it to that of ext2 installed on HDD and SSD. The extent sizes of MatBall are 64KB and 256KB and $\lambda = 16.$ As can be seen in the figure, the write performance of ext2 on HDD is much lower than that of MatBall because of the hybrid structure of MatBall.

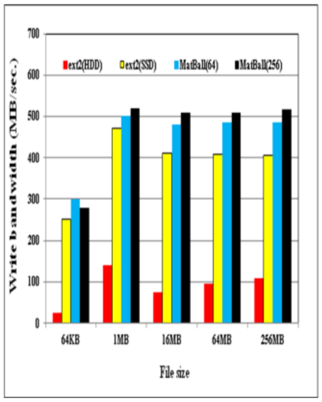


Figure 4. Write $\lambda = 16$

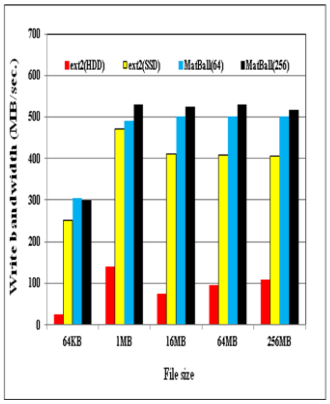


Figure 5. Write $\lambda = 32$

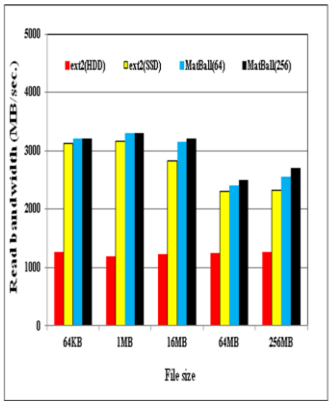


Figure 6. Read $\lambda = 16$

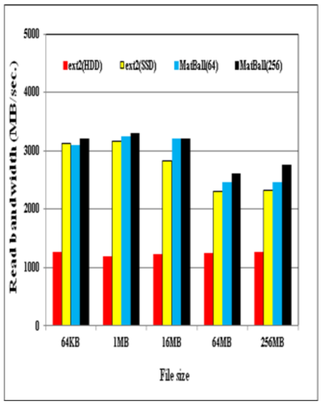


Figure 7. Read $\lambda = 32$

When the write throughput of MatBall composed of 64KB of extents is compared to that of ext2 installed on SSD, with 256MB of file size, there is about 19% of performance improvement. This is because MatBall uses the large I/O units for write operations.

The advantage of using the large I/O granularity is also observed in the write performance of MatBall composed of 256KB of extent sizes. The figure shows that MatBall using 256KB of extent sizes produces about 6% performance improvement compared to MatBall with 64KB of extents.

However, in write operations on small files such as 64KB of files, using the larger extent size does not produce the performance speedup. According to Figure 4, on top of 64KB files, using 256KB of extent size rather decreases the write performance, when compared to using 64KB of extent size. This is because of the overhead for coalescing data on extents. In other words, with small files, the larger the extent size is the more the overhead for collecting data on extents takes place. However, on top of large files, writing with the large I/O granularity increases the write throughput due to the reduction in I/O accesses.

Figure 5 shows the write performance with $\lambda = 32$. Since the file sizes of IOzone are aligned with extent sizes, no remaining blocks on extents are left posterior to file allocations. As a result, only the segment partitioning on the top level takes place for both extent sizes.

For example, with 64KB of extent sizes, only seven segments on the top level are configured and used for file allocations. Every file size uses the entire 64KB of extents although multiple extents are used for files larger than 64KB. Therefore, no segment partitioning is needed to reuse extents. The same I/O behavior can be observed with $\lambda = 16$ in Figure 4. As a result, there is no noticeable difference between the write performances with $\lambda = 32$ and that of $\lambda = 16$.

Figure 6 and 7 show the read performance with $\lambda = 16$ and with $\lambda = 32$, respectively. In this case, we can see that the memory cache significantly affects in the read performance. Figure 6 shows that the prefetching scheme implemented in ext2 offsets the performance difference caused by device characteristics a little. Because the difference of the read performance between ext2 on HDD and ext2 on SSD is lower than that of the write difference of ext2 between two devices.

Likewise, we cannot find the noticeable difference between MatBall with 64KB of extent sizes and that with 256KB of extent sizes. However, because of the less read accesses, on top of 256MB of file sizes, using 256KB of extent sizes produces 5% of performance speedup over 64KB of extent sizes. Also, in Figure 6 and 7, we can see that changing the threshold value for the segment partitioning does not effect on the read performance because read operations are not involved in the segment partitioning.

IV. CONCLUSION

The main goal of MatBall is to increase the space utilization of SSD partition in the hybrid file system where the entire address space is provided by integrating a small portion of SSD partition with a much larger HDD storage capacity. MatBall tries to consume the remaining spaces as much as possible posterior to file allocation processes, by recursively partitioning segments in the subsequent level and by allowing the further file allocations on the partitioned segments. We evaluated MatBall using IOzone. When file sizes are either a multiple of extent sizes or larger than the extent size, the segment partitioning to the lower level does rarely take place. In this case, the threshold value for the segment partitioning in MatBall does little affect I/O performance. On the other hand, with a large number of small-size files, MatBall can improve I/O bandwidth by converting data into the larger I/O granularity. As a future work, we will verify the effectiveness and suitability of file allocation method of MatBall by using various applications.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIP)(NRF-2014R1A2A2A01002614).

Also, this work was supported by the Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government(MSIP) (No.B0101-15-0548(2016), Development of Ultra Power-Saving and High Integrated Micro Server Technology for Cloud Infra).

REFERENCES

[1] N. Agrawal, et al., “Design Tradeoffs for SSD Performance,” In Proceedings of USENIX Annual Technical Conference, pp. 57-90, June 2008.

[2] M. Saxena, M. Swift, and Y. Zhang, “FlashTier: a Lightweight, Consistent and Durable Storage Cache,” In Proceedings of EuroSys’12, pp. 267-280, 2012.

[3] C. Wu, H. Lin, and T. Kuo, “An Adaptive Flash Translation Layer for High-Performance Storage Systems,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 29, pp. 953-965, 2010.

[4] A. Rajimwale, V. Prabhakaran, and J.D. Davis, “Block Management in Solid-State Devices,” 2009 USENIX Annual Technical Conference, pp. 21-26, June 2009.

[5] H. Kim, S. Seshadri, C. Dickey, and L. Chiu, “Evaluating Phase Change Memory for Enterprise storage Systems: A Study of Caching and Tiering Approaches,” In Proceedings of the 12th USENIX conference on File and Storage Technologies, Santa Clara, USA, pp. 33-45, 2014.

[6] W. Josephson, L. Bongo, K. Li, and D. Flynn, “DFS: A File System for Virtualized Flash Storage,” ACM Transactions on Storage, Vol. 6, No. 14, pp.1-15, Sept. 2010.

[7] C, Lee, D. Sim, J. Hwang, and S. Cho, “F2FS: A New File System for Flash Storage,” In Proceedings of the 13th USENIX conference on File and Storage Technologies, Santa Clara, USA, pp. 273-286, 2015.

[8] J. Kang, et al.,“SpanFS: A Scalable File System on Fast Storage Devices,” In Proceedings of USENIX Annual Technical Conference, Santo Clara, USA, pp. 249-261, 2015.

[9] C. Li, et al., “Nitro: A Capacity-Optimized SSD Cache for Primary Storage,” In Proceedings of USENIX ATC’14, Philadelphia, USA, pp. 501-512, 2014.

[10] P. Huang, P. Subedi, X. He, S. He, and K. Zhou, “FlexECC: Partially Relaxing ECC of MLC SSD for better cache performance,” In Proceedings of USENIX Annual Technical Conference, Philadelphia, USA, pp. 489-500, 2014.

[11] Z. Zhang and K. Ghose, “hFS: A Hybrid File System Prototype for Improving Small File and Metadata Performance,” EuroSys’07 , pp. 175-187, 2007.

[12] E.Gal and S. Toledo, “A Transactional Flash File System for Microcontrollers”, In Proceedings of the USENIX Annual Technical Conference, pp. 89-104, April 2005.

A Study on Information System for Science of Science and Technology Policy

Seung Su Chun
Division of Information & Knowledge
Korea Institute of S&T Evaluation and Planning
Seoul, South Korea
dabins@kistep.re.kr

***Abstract*—As social, economic, and cultural environments have rapidly been changing, uncertainties and complexities have also increased with regard to research and development projects. Issues are across various fields and interconnected with different problems, which makes it harder to plan and design R&D projects and to estimate their effects as well. Linear and sequential approaches are not appropriate to deal with these changes. Rather, circular and simultaneous perspectives with more precision and rigor are needed. To this end, more information should be gathered and all parties concerned should be required to cooperate. It becomes essential to establish a science's evidence based and integrated system supported by all parties concerned for high quality and effective policy making.**

Keywords-Technology Policy, Decision Making System, Knowledge, R&D management

I. SCIENCE OF SCIENCE POLICY

Some of the advanced countries have recognized challenges and started to run a variety of programs such as science of Science and Innovation Policy to create the 3rd generation innovation systems for science and technology. The concept and term of Science of Science and Innovation Policy was first brought up and coined by Dr. Marburger of American Association for the Advancement of Science (AAAS) in 2005. This was based on the recognition that it is indispensable to understand complex relationships between R&D investments and innovation together with their consequent improvements of competitiveness and social benefits for policy effectiveness [1].

Among governing bodies attempting to make policy decisions scientific are Science of Science and Innovation Policy(SciSIP) of the US and European Innovation Scoreboard(EIS) and European Research Area WATCH of EU. Value-based technology innovation such as 'knowledge intensification and creative design' becomes more important in securing competitiveness of businesses and nations. All these factors increase the needs for IT infrastructure and in-depth studying of intellectual business system which support policy decision making based on scientific evidence [2].

However, the linear approaches to technological innovation model and policy supporting instruments so far have clear limitations to effectively deal with these technical changes and complex issues.

II. DESIGN OF DECISION MAKING SUPPORT SYSTEM

Current researches has stemmed from systems dynamics based on systems theory and feedback thinking, and evolved into cybernetics and automatic control mechanism. Interdisciplinary researches on new models of knowledge-based dynamics and policy aid have been required more than ever as high-technologies have converged and policy management system has changed [3]. In this paper, we propose mechanisms to achieve the service provision of Science of Science Policy. For this purpose, current processes are analyzed to identify factors, which need to be improved and analytical methodologies are also defined [4]. Then, major components are developed to effectively support the processes according to each methodology [5]. Evidence-based knowledge is utilized in the activities of policy adoption, implementation, and evaluation including decision-making [6]. When designing specific integration models, each Situation(S) is represented by unit of Topic(T), which equals Term(T) used in natural language. The integration model conducts text-mining by processing all documents and texts within the system into natural language, resulting in abstracting representative terms. This generates a knowledge model through analysis of relations between topics and layered structures of resources. Related to processes and tasks of the knowledge model, an Address of document repository is defined as a process and Task is defined as a name of the specific document directory.

The model which generates knowledge models automatically is defined as below:

Policy Making Supporting Model：M = {Process, Task, Resource}

Process：P = Document Repository {Address$_1$, ... Address$_n$}

Task：T = Document Directory {Name$_1$, ... Name$_n$}

Resource Element：Topic：E = Mining {Term$_1$, ... Term$_n$}

A component of a process is defined as task flow and relation and is designed so as to combine an integrated information system and service. With regard to collection of

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-503-6

policy information, information has been collected on the basis of a component supporting tasks. Knowledge base integration of policy information has progressed through structuration of task-specific data and information as shown in Table I.

TABLE I. CONFIGURATION OF SYSTEM

Process	Components
Technology Policy	-Integrated information retrieval and Management -Technology monitoring / Trend analysis on a real time basis -Combined wire-wireless service
Forecasting	-Community for future prediction -2D matrix Delphi survey -Visualization of Roadmap
Planning	-Medium and long-term plans, database on policy trends, other data query
Investment strategy	-DB for investment planning on a micro level and process supporting -Project analysis and management -Links to information on R&D programs
Validity analysis	-Benefit analysis of R&D -Instruments for ripple effect analysis -Instruments for cost/paper analysis
Investigation analysis	-Unified search function for statistical indices -DB of statistical tables and graphs
Program coordination	-Program track records / Budget planning supporting -Budget requests, DB of mid-term project plans and deliberation materials
Program evaluation	-Query for in-depth evaluation results -Expert committee management

III. SYSTEM DEVELOPMENT

Specific policy processes and task connection models are needed for effective service structure, and integrated process maps should be designed to address components and information such as for example data and documents. The service of Science of Science Policy aims to improve the efficiency and reliability of producing policy alternatives. It is very important that while utilizing massive data and sharing instruments, we analyze various functions. Therefore, a component-based development method is appropriate and it should be comprised of unitary system for organic combination of the services. For example, various reference information is needed on fields, stages, and targets to be used both as a forecasting basis and for validity analysis. However, a particular expert or outdated data have been the only materials that policy community has depended on. Improved science policy support systems cause improvements in the effective activities of the proportion of researchers with the report, as shown in Table 2. Thus, the new service for technology analysis helps produce more objective and timely materials of technology value analysis and validity analysis through information on technology trends and massive database analysis on publication, patents, and market as shown in Table 3. For this reason, the database we reference provides 2.68 million data on publication, patents, and market and analysis of 0.34 million items of documents on policy trends.

TABLE II. RELATED DATA OF INNOVATION POLICY

Activity	Current	Improved	Change
Ration of searchers	28.8%	48%	+19.2%
researchers n tasks	32	55	+71%
improvement	2	7	+250%
Num. of reports	85	102	+20%
R&D projects	1.5	2.2	+46%
per researcher	0.2	0.3	+50%

TABLE III. RELATED DATA OF INNOVATION POLICY

Patents	Market	Statistics	Total
2,608,385	2,151	129	2,681,546
Knowledge analysis	Prediction experts	Validity experts	Evaluation experts
3,242	1,030	298	2,425

IV. CONCLUSIONS

This study has established an integrated knowledge base of policy support for the service of Science of Science Policy by standardizing and specifying processes. This approach has required organizing and comprising the specific functions on a basis of component units according to demand from stakeholders such as major information demanders, its users request patterns and policy decision makers. In turn, these works have made it possible to create the service of Science Policy which can control major policies on a real-time basis by catching and tracking policies' current states in the processes of adopting, implementing, evaluation and thus support evaluation and coordination of them based on objective data.

REFERENCES

[1] OECD/GD102, "Knowledge based Economy", organization for economic co-operation and development, OECD, 1996

[2] E. Feigenbaum, P. M. Corduck, "Integrating knowledge into computer systems", Second citation, wikipedia.org, 2010

[3] V. Devedzic, "Knowledge Modeling - State of the art", Integrated CAE, vol. 8, pp. 257-281, 2001

[4] P. Braunerhjelm, "An Innovation Policy Framework: Bridging the gap between industrial dynamics and growth", EPSE, Springer, Vol. 34, pp 95-130, 2016

[5] John E. Hanke, Dean W. Wichern, "Business Forecasting", Pearson Education Press, Eighth Edition, pp.57, 2005

[6] Robert J. Thierauf, "Optimal Knowledge Management", IDEA Group Publishing, pp.89, 2006

A Framework for Anonymous Communication in MANETs based on Access Control and Authenticated Key Agreement

Ehab E. Zakaria
Faculty of Computer Science
MSA University
Giza, Egypt
e-mail: ezakaria@msa.eun.eg

Haitham S. Hamza Imane A. Saroit
Faculty of Computers and Information Sciences
Cairo University
Cairom Egypt
e-mail: hhamza@fci-cu.edu.eg, i.saroit@fci-cu.edu.eg

***Abstract*—Mobile ad hoc networks (MANETs) are finding ever-increasing applications in both military and civilian systems owing to their self-configuration and self-maintenance capabilities. Communications in battlefields and disaster recovery are other examples of application environments. Many of these applications are security sensitive. As a result, security in MANETs has recently been drawing much attention. The vast majority of existing solutions that provides security services for MANETS does not take into consideration the need for authentic access control mechanism as a first line of defense to ensure that only the eligible nodes are involved. In this work, we propose an anonymous communication scheme that is based on an efficient access control mechanism with authenticated key establishment. Besides service integration offered by this framework, simulations and analysis showed that the proposed solution enhance quality of service (QoS) level compared to the existing approaches that aims to provide only access control or anonymous services separately. With a similar or a lower cost, our integrated approach enhanced MANET security and performance in comparison with other related proposals.**

Keywords—MANET; Anonymous communication; Access control; Identity-based cryptography

I. Introduction

Mobile ad-hoc networks (MANETs) are an ideal technology to deploy spontaneous wireless infrastructureless networks, either for military or civilian applications.

Throughout recent years, MANETs have gripped a lot of attention due to its dynamic nature to establish wireless networks of mobile nodes and wireless routers. The key advantage of ad-hoc networks is that the knowledge about network topology is not necessary and even more it’s not necessary to have an infrastructure. Without any centralized entity ad-hoc networks are able to operate in an autonomous and spontaneous manner. Also all the required network modifications will be done in a self-configurable way.

In order to have a proper function for a mobile ad-hoc network and achieve cooperation among all networking nodes, it is necessary to limit network access of packet forwarding and routing to righteous nodes and reject access from misbehaving nodes. However, the network access protocols commonly used in traditional infrastructure-based networks are not applicable in MANETs due to the lack of fixed infrastructure, frequent changes in topology and node membership, and finally due to the potential attacks from adversaries inside the network itself [1]. This situation enforces the need to develop different strategies that suit MANET architecture in order to deploy an efficient access control mechanism.

Also, the privacy of communication and sensitive information has become a serious issue on the Internet. Encryption schemes shield the contents of communication, but do not hide the fact that two users are communicating. In many situations, users may need to make their communication anonymous. Sensitive information includes the identities of communicating parties, network traffic patterns [2]. The leak of such information is often disturbing in security-sensitive situations. For example, an unexpected change of the traffic pattern in a military network may indicate a forthcoming action, a chain of commands, or a state change of network alertness [3]. It may also disclose the locations of command centers or mobile VIP nodes, which will enable the enemies to launch pinpoint attacks on them. In contrast to active attacks, which usually involve the launch of denial of service or other more “visible” and hostile attacks on the target network, traffic analysis is a kind of passive attack, which is “invisible” and difficult to detect. It is therefore important to design countermeasures against such malicious traffic analysis, which leads to the importance of deploying an efficient mechanism that ensure communication anonymity in MANETs.

In this paper, we address two main concerns in MANETs; namely access control and anonymous communication in order to provide a framework for secure communication. Most of the work done only provides separate solutions for each of the two issues, putting into consideration the vitality of the two services as a backbone for secure MANET operations. For real life situations, a

MANET administrator should deploy the two services separately each with its independent cost. In comparison to other monotonic solutions that only provides one service at time, we argue that with a similar or even lower cost the security services can be highly correlated in a single framework that provides MANET nodes with key management, access control and anonymous communication capabilities.

The rest of this paper is organized as the follows. In Section 2, we provide a background for access control and anonymous communication in MANETs and the major proposals that dealt with them. In Section 3, we present the preliminaries that are utilized in developing our proposed solution including elliptical curve with pairing and threshold secret sharing basics. In Section 4, we specify the network model, and the adversary model for the framework design. In Section 5, we present our proposed framework. In Section 6, we provide a performance analysis for our framework in comparison with existing solution.

II. RELATED WORK

Most of the work provided in the literature provides separate solutions for access control and anonymous communication schemes; here we provide a background for each of them.

A. Access Control

Access control for MANETS is a challenging task for a number of reasons [5]:

- First, MANET environment is a distributed problem. It does not have a clear defense line like other types of networks (wired or cellular) which make it difficult to implement the access control mechanism at routers or base stations.
- Second, it's preferable that any access control service will be available at each node locally in order to evade communication over unreliable multihop channels.
- Third, access control solutions should deal with nodes' misbehavior, as network nodes could already hold access control information.
- Finally, as node membership in MANET has a dynamic nature, the solution has to dynamically deal with that.

Kim et al. in [6] presented an early effort to build a framework for network access control using cryptographic techniques and protocols. Their framework classifies admission policy based on the entity which makes the admission decisions (external or internal entity). Despite of, the simplicity and the relative easiness to support these polices, they are inflexible and unsuitable for MANETs.

Zhou and Hass [7] proposed using threshold cryptography [8] to secure MANETs. They suggested distributing CA's (Certificate Authority) public key to each node, while CA's private key distributed among the subset of nodes such that a certain threshold of them can jointly perform certificate generation to the nodes joining the network.

Saxena et al. [9][10] make use of various existing threshold signature schemes to build a distributed admission control mechanisms for ad-hoc groups, but, they did not tackle the problem of group membership revocation.

B. Anonymous communication

Throughout the literature, a number of anonymous communication protocols have been suggested. Most of them come from Chaum's two important approaches: mixnet [11] and DC-net [12]. These protocols discussed three types of anonymous communication properties: sender anonymity, recipient anonymity and relationship anonymity.

- **Sender anonymity:** means that a particular message is not linkable to any sender and no message is linkable to a particular sender.
- **Recipient anonymity:** similarly means a particular message cannot be linked to any recipient and that to a specific recipient, no message is linkable
- **Sender-recipient relationship anonymity (or relationship anonymity in short):** refers to that the sender and the recipient cannot be marked as communicating with each other, though it may be clear they are participating in some communications.

The mixnet family protocols (e.g., [13][14]) make use of special servers that intended to shuffle the received packets to make the communication path (including the sender and the recipient) unclear "ambiguous" these servers called "mix" servers. In order to achieve the desired anonymity, these protocols depend on the statistical features of the underlying traffic which is also called cover traffic. As a result, these protocols are inadequate in dynamic network environments like MANETs where trusted servers are unavailable.

The DC-net family protocols (e.g., [15][16]) use secure multi-party computation techniques. They offer verifiable anonymity without depending on trusted third parties. However, these protocols have transmission collision problem which does not have a concrete solution.

III. PROPOSED FRAMEWORK

The majority of solutions provided to address security of mobile ad-hoc networks only tackle one concern at a time either it be access control, key management, secure routing, anonymous communication, etc. Our proposed framework aims to provide three of the major security services that we believe in its importance in order to provide a concrete and solid secure framework for MANET operations. Our proposed framework provides key management, access control and anonymous communication and secure in a single coherent framework. We firstly introduced this framework at [17] utilizing the proposed identity based cryptography and access control techniques to provide crucial MANET services, namely address auto-configuration, secure pairwise communication and secure group communication. The main advantage of this framework that it provides the mentioned services without adding an excessive computational or communication overhead compared to existing solution that provides only one of our services. Our proposed anonymous communication scheme is based on an efficient access control mechanism with authenticated key establishment using identity based cryptography and threshold secret sharing techniques.

Our mechanism provides its services without any assumption of a prefixed trust relationship between nodes, which effectively resolves the problem of single point of failure in the traditional public key infrastructure. In this paper, we present an access control mechanism based on the usage of membership access ticket using identity based cryptography primitives. Based on the possession of a valid access ticket, mobile nodes can get involved in a secure communication achieved through our proposed anonymity protocol.

We consider a MANET consisting of *N* nodes, and the network size may change dynamically as nodes may join, leave, or crash at any time. Each node has a unique non-zero ID and assumed to be its MAC address. In order to improve system efficiency in terms of communication and computation, we employed identity-based cryptography (IBC) as an efficient alternative to the traditional public key cryptography techniques to provide essential cryptographic primitives.

Fig. 1 depicts our framework, at the top layer, resides the three main services; access control, anonymous communication which are based on the intermediate layer that provides the key management functionality using IBC primitives provided by the lower layer. Hereafter we describe protocols used to provide our targeted services.
We propose four algorithms that provide collectively the functionality of key management, access control and anonymous communication.

A. Key Management and Access control

Key management functionality in terms of the creation of master public key, master private key share, nodes private key and new master private key share creation for a new node are accomplished through algorithms 1 , 2 and 3. Access control functionality is accomplished based on key management and appears in algorithm 2.

For membership renewal, after the membership access ticket (MAT) of a certain node expires, it sends a request to **K** neighbor nodes, where each of them checks node's behavior, then send signed partial membership token. The requesting node combines partial signature to acquire its new MAT. Nodes behavior observation is out of our scope.

Membership revocation of MAT happens for one or more of the following reasons:

1. Due to expiry of MAT.
2. Due to misbehaving or selfishness.

B. Privacy and Anonymous Communication

It's widely known that privacy is conflict with authentication and certification which achieved only through a trusted third party (TTP) registration but in order to trace any node that would give out false information there must be a registration. Hence when node X transmit a message to node Y, Y needs to check that X is a registered and authenticated node through the certificate that escort the message X, so that any node can be traced if the need arises. The certificate must be signed using certificate authority (CA) private key in order to enable Y to check the validity of the certificate. But in order to protect communicating entities privacy any message sent by one party should appear as if sent by another entity so that pseudonyms are needed, however the pseudonyms should contain some information that let the CA (and only the CA) to determine the true identity of its holder.

Algorithm 1 describes the steps carried out by network nodes in order to cooperatively produce system's master public key based on elliptic curve cryptography (ECC). Based on the concepts proposed by Pedersen [18], we employ ECC to generate the master public key and private key share. In our proposed scheme we operate without any trusted authority support, where the master key pair is computed jointly by the initial network nodes.

Algorithm 1: *Master Public Key and Master Private Key share generation*

```
1. Each node $\mathbf{n_i}$ randomly chooses a secret $\mathbf{x_i}$ and a polynomial $\boldsymbol{f_i(z)}$ of degree k-1, s.t: fi(0)=xi.
2. Each node ni compute its sub-share for $\mathbf{n_j}$ as SSij= $\boldsymbol{fi(j)}$, j=1,2,3,...
3. Send $SS_{ij}$ securely to $\mathbf{n_j}$.
4. After receiving n-1 sub-shares $\mathbf{n_j}$ compute its share of master private key as $S_j=\sum_{i=1}^{k} SS_{ij}$
5. Any coalition of K nodes can recover the secret using $\sum_{i=1}^{k} S_i l_i\,(z) \bmod q$ where $l_i(z)$ is Lagrange Coefficient.
6. Each shareholder publishes $S_iP$, where P is a common parameter used by IBS. $S_iP$ is a point multiplication.
7. Master public key $\mathbf{Q_n}=\sum_{i=1}^{k} \mathbf{S_i\ P}$
```

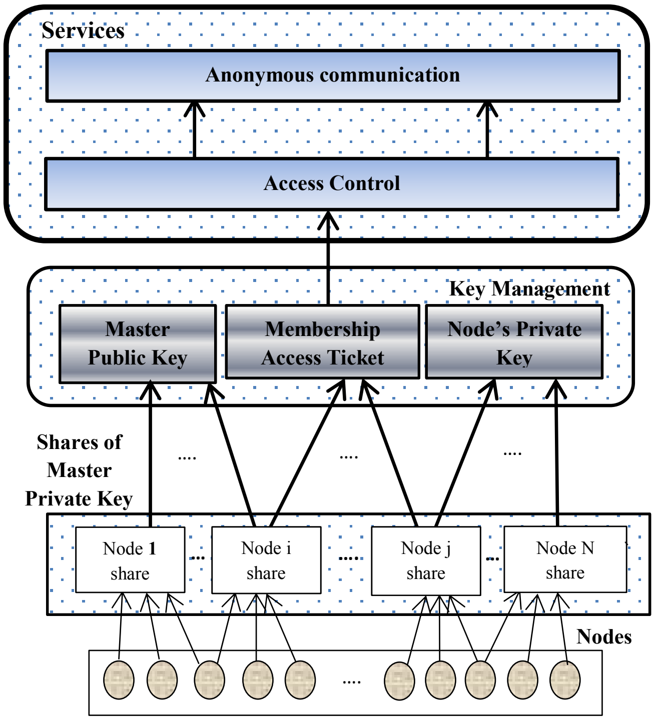


Figure. 1. Proposed Framework.

Algorithm 2 describes the proposed node's private key and access ticket generation process which is the core used to provide access control and anonymous communication services in our frame work. For a node J, in order to get its private key and acquire a ticket that can be assumed as its access key to the network, we assume that, node's J public key (representing node's identity) is the hash value of its MAC address. Then node J should contact at least k of its neighbor nodes presenting its identity (identity-based cryptography) and request private key generation service (PKG) (*if J was unable to find k neighbors locally, node J would move (roam) to another location*). Since all network nodes share the master private key, any node can be a service node.

Each of k nodes generates a share of the new private key SK_{ij} and sends it to node j, which in turn combine all the shares to generate its new private key SK_j. For authentication, as the new node joins the network it presents any required physical proof. And upon authentication by any *t* nodes, each node of them generate a partial membership access ticket MAT_j^i using its share of the master private key S_i on on the public key of the node appended with the expiry time of this ticket $\mathrm{Exp\_time}_j$ and its issuing time T_j.

Upon reception of partial tickets node J combines then in order to get its access ticket MAT_j. Using MAT_j node J can participate in further network actions and services

.

Algorithm 2: *Private Key and access ticket generation*

```
1. Node **J** Public key $Q_j$=H (MAC_ADD).
2. Node **J** Contact at least k nodes and get $SK_{ij}=S_iQ_j$ .
3. Node **J** compute its private key as $SK_J= \sum_i^k S_i Q_j$
4. Upon authenticating the new node (maybe using some physical proof) by any **t** nodes of the **k**
    a. Each node **i** Issue a partial membership access ticket (**MAT**):
           $MAT_j^i = S_i(Q_j||\mathrm{Exp\_time}_j||T_j)$
    b. Node **J** combine partial tickets as
           $MAT_j = \sum_{i=1}^t S_i \mathrm{H}(Q_j||\mathrm{Exp\_time}_j||T_j)$
```

Algorithm 3 describes steps carried out to enable a new node n to get a new share of the master private key, in order to participate in network services. Any coalition of K existing nodes can jointly participate in the process. Each of the participating nodes create a partial share $S_{i,n}$ and send it to the new node which accumulate those shares in order to get its share of Master Private Key.

Algorithm 3: *New Master Private Key share creation for new node n*

```
1. Each node **i** of **k** generate partial share as $S_{i,n} = S_i l_i(n)$,
       $l_i(n)$ is Lagrange coefficient.
2. Each node **i** send the share to node **n**.
3. Node **n** adds shares to get $S_n = \sum_{i=1}^k S_{i,n}$
```

So, the true identity of a node should not be known or readable to any other node. A certified authority (or a trusted party) should sign the pseudonym to ensure that it has a trusted signature in order to achieve privacy and authentication. In order to overcome limitations imposed by CA-based architecture, we armed our security framework with an anonymity and privacy features through the usage of the proposed security architecture that utilize identity based cryptography and threshold cryptography in order to the achieve security goals.

Since that our proposed framework's design supports services flow, the privacy and anonymity features are built upon the ability of the node to have a righteous access control through steps accomplished through Algorithm 1 and algorithm 2.

In our proposed anonymity solution, for two parties **Alice** and **Bob** to communicate anonymously they use pseudonyms to conceal their identity as **Carol** and **Dale. Alice** starts with creating an alias identifier rather than its true identity as **Carol,** with this it creates an alias public key (**PK$_{\mathbf{als}}$**) and its corresponding alias private key (**PrK$_{\mathbf{als}}$**). Then perform the following steps described in algorithm 4.

```
Algorithm 4: Privacy and Anonymous Communication

1. Alice generate an alias id (carol) , alias public key ($PK_{als}$) and alias private key ($PrK_{als}$)
2. Alice sign its $MAT$ with its system generated private key $SK_{alice}$ as its original certificate Original_Cert = $SIG_{SK_{alice}}(MAT_{alice})$
3. Alice encrypt Original_Cert combined with its system public key $Q_{alice}$ and a timestamp $TS$, with system master public key $Q_n$, producing a system authenticator Sys_Auth= $E_{Q_n}$ ($Original\_Cert$ || $Q_{alice}$ || $TS$), TS change each time to make Sys_Auth looks different each time.
4. Alice send a message M = (PK_als, Sys_Auth, $SIG_{PrK_{als}}$( H(entire_message)) to K nodes for a partial signature.
5. Each of the K nodes, checks signature correctness using PK_als and sign the digest of the message (PK_als, Sys_Auth) using its share of the master private key $S_i$ and return it to carol (Alice)
   Note: none of the signing nodes can know the identity of the requesting node (Alice), all it do that it sign on the combination Sys_auth and PK_als and that they belong to the same identity.
6. Alice combine the received partial signatures to make its Alias_Cert as the same way a new node gets its private key (algorithm 2).
      Alias_Cert =$\sum_1^k S_i$ (Life_Span, PK_als, Sys_Auth)
7. To send a message to bob;
   i.   Carol (Alice) sign the digest of the message with its alias private key.
        Signed_Hash=$SIG_{PrK\_als}$(H(message)||TS)
   ii.  Carol (Alice) send the message as:
        [Alias_Cert || Signed_Hash || message]
8. For privacy, the message can be encrypted with intended recipient public key (bob).
For Bob when he receives the message:
   1. Use system public key $Q_n$ to verify signature on carol's certificate.
   2. If carol's certificate is valid PK_als is considered authentic and used to authenticate (verify) signature on carol's signed hash to get [H(message)||TS]
   3. If message is encrypted using Bob's alias PK, he uses his alias private key to decrypt the message.

For Bob to replay as Dale:
   1. Do the same steps to get his alias certificate.
   2. Send [Dale's Certificate|| H(carol's message) || Dale's Signed hash || Dale's Message or $E_{PK_{als}}$ (Message)]
```

In case of the existence of a misbehaving node, our model requires the existence of some arbitrator or some reference entity to manage resolving the issue. If a threshold number of nodes (*R*) complain about an anonymous node (*X*), then this node is stripped out of its anonymity to find out its true identity to take the proper actions against. In order to resolve the dispute, a need to reveal the true identity of a misbehaving node (ex. carol) is aroused, and the following steps are carried out:

1. The arbitrator decrypt carol's certificate (*Alias_Cert*) using system public key Q_n D_{Q_n} (*Alias_Cert*)= [Life_Span, PK$_{als}$, Sys_Auth]
   The arbitrator decrypt **Sys_Auth** by sending it to ***K*** nodes where each node uses its share of the master private key and the arbitrator combines the responses.
   $\sum_1^k D_{S_i}$ (E_{Q_M} (**Sys_Auth**)) = [$Original\_Cert$ || Q_{alice} || TS]

2. The arbitrator decrypt ***Original_Cert*** using Alice's public key $\boldsymbol{Q_{alice}}$ derived from the decrypted **Sys_Auth** in order to prevent false accusations $D_{Q_{Alice}}(\boldsymbol{SIG_{SK_{alice}}}$ $(MAT_{alice})) = MAT_{alice} = \sum_{i=1}^{t}$ S_i H(Q_{Alice}|| Exp_time$_{Alice}$)

TABLE 1. COMPARISON WITH EXISTING PROTOCOLS

	Sender Anonymity			Recipient Anonymity		Overhead	Latency
	External Nodes	*Internal Nodes*	*Recipient*	*External Nodes*	*Internal Nodes*		
OR	√	√	**NO**	√	√	O(I)	O(I)
BUS	√	√	√	√	√	O(N^3)	O(N)
CROWDS	√	√	**NO**	√	**NO**	O(d)	O(I)
KMAT	√	√	√	√	√	O(N^3)	O(N)
Proposed	√	√	√	√	√	**O(N^2)**	**O(N)**

ISBN: 978-1-61208-503-6

3. Check $\widehat{e}(Q_n, H(Q_{Alice} \,||\, \text{Exp\_time}_{Alice})) \equiv \widehat{e}(P, MAT_{Alice})$

If the above condition is true, then Alice identity is confirmed, and it is impossible for any other node to use Alice identity for malicious actions.

IV. Performance Analysis

As stated earlier existing security solutions for MANET provide security services separately. In our pervious papers [17] we provided a detailed performance analysis for our proposed framework in terms of access control and key management. In this Section, we provide a performance analysis for the integrated protocol for anonymous communication.

A. Comparison with Some Existing Schemes

We provide here a comparison for our proposed protocol with some existing solutions for anonymity in MANET, namely OR[19], Crowds[20], BUS[21], KMAT[22].

Like mixnet-based protocols (OR, Crowds), our proposed solution provides anonymity to the sender and the receiver. Also they do not account on the statistical characteristics of the underlying traffic. Both hide the sender and the receiver from each other. Our proposed solution is more efficient than BUS in terms of overhead as our solution is O(N^2) while BUS is O(N^3), where N is number of the nodes in the network. And unlike BUS our solution permits the receiver to reply without able to identify sender identity and provides broadcasting messages anonymously.

In comparison to KMAT, our proposal achieves the same level of anonymity with a lower communication overhead.

Table 1 shows a comparison in terms of latency and overhead between our proposed solution and the existing ones (where *I* is the number of intermediate nodes, and *N* is the number of the nodes in the network). We can conclude that the proposed solution provides an enhanced anonymity in comparison with current anonymous communication protocols, where with the same or less communication overhead it provides the same anonymity level.

B. Security analysis

Our solution achieved the three types of anonymous communication properties:

- **Sender anonymity**: where none of the transmitted messages can be linked to any sender.
- **Recipient anonymity:** where none of the messages can be linked to a certain recipient
- **Sender-recipient relationship anonymity**: Even it may be clear that two entities are involved in a communication, but they cannot be identified as communicating with each other.

Those three anonymities called full anonymities, as an attacker cannot infer any knowledge about the a sender, a receiver or the communicating parties of any transferred messages from a current traffic

V. Conclusion

In this paper, we proposed a secure anonymous communication scheme for MANETs based upon authenticated access control mechanism that ensures the proper behavior within MANET as only nodes with rights to access the network will be involved, which enhances the reliability of the other security functions. The proposed scheme has many advantages over existing solutions as it provides a concrete framework for access control, key management and anonymous communication based on ideas from threshold secret sharing and ID-based cryptography. As results shows the proposed scheme is more efficient than the previously proposed solution for anonymity in addition to the extended capabilities of the proposed framework which also support access control and key management services which can be further extended to provide more security service for MNAETs. Due to the usage of threshold and identity based cryptography our proposed framework exhibits an optimized performance feature. Throughout this work we showed how we can enforce access control through making it a mandatory component in order to get access to other services like anonymous communication. The deliverables from the access control stage is used as a key in the subsequent stage in a way that make smooth service integration. Measurement results and performance analysis indicate that our solution provides an integrated framework for secure communication with an overall performance that outcome existing solutions, which make it more suitable in MANET environment.

References

[1] L. Haiyun, K. Jiejun , P. Zerfos and L. Songwu, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks", Networking, IEEE/ACM Transactions on (Volume:12, Issue: 6), pp.1049-1063, 2004.

[2] Lou and Y. Fang, "A Survey on Wireless Security in Mobile Ad Hoc Networks: challenges and available solutions", Book chapter in Ad Hoc Wireless Networking, Kluwer, pp. 279–294, 2009.

[3] Y. Kim, D. Mazzocchi, and G. Tsudik, "Admission Control in Peer Groups," IEEE International Symposium on Network Computing and Applications (NCA), pp. 104-113, 2003.

[4] DARPA. Research Challenges in High Confidence Networking. July 1998.

[5] B. Qing-hai , Tongliao, “Comparative research on two kinds of certification systems of the public key infrastructure (PKI) and the identity based encryption (IBE)”, Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), pp. 147 – 150, 2012.

[6] L. Zhou and Z.J. Haas, “Securing ad hoc networks”. IEEE Network, vol. 13, Issue 6, pp. 24–30, 1999.

[7] Shamir, “How to share a secret”. Communications of the ACM, volume 22, issue 11, pp. 612–613, 1979.

[8] N. Saxena, G. Tsudik, and J. H. Yi, “Access Control in Ad Hoc Groups” International Workshop on Hot Topics in Peer-to-Peer Systems (HOT-P2P), pp. 2 – 7, 2004.

[9] N. Saxena, G. Tsudik, and J. H. Yi, “Threshold Cryptography in P2P and MANETs: The Case of Access Control,” International Journal of Computer and Telecommunications Networking, vol. 51, issue 12, pp. 3632-3649, 2007.

[10] D. Chaum, “Untraceable Electrical Mail, Retrun Address, and Digital Pseudonyms”. Communications of the ACM, volume 24, issue 2, pp. 84–88, 1981.

[11] D. Chaum, “The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability”. Journal of Cryptology, volume 1, pp. 65–75, 1988.

[12] C. Huseyin, “Anonymous Communications in Mobile Ad Hoc Networks”, Phd-Kongens Lyngby, 2006.

[13] M. Reiter and A. Rubin, “Crowds: Anonymity for Web Transaction”. ACM Transactions on Information and System Security, volume 1, issue 1, pp. 66–92, 2000.

[14] L. Ahn, A. Bortz, and N. Hopper, “K-anonymous message transmission”. In Proceedings of the 10th ACM conference on Computer and Communications Security, Washington D.C., USA, pp. 122–130,2003.

[15] P. Golle and A. Juels, “Parallel Mixing”. In Proceedings of the 11th ACM Conference on Computer and Communications Security, Washingto D.C, USA, pp. 220-226, 2004.

[16] Ehab E. Zakaria., H. S. Hamza, and I. A. Saroit, "An Integrated Security Framework for Access Control and Address Auto-configuration for MANETS", WMNC 2015, 8th IFIP Wireless and Mobile Networking Conference, Minich, Germany, pp. 253 – 260, 2015.

[17] T. P. Pedersen, “A Threshold Cryptosystem Without A Trusted Party,” EUROCRYPT, pp. 522-526, 1991.

[18] P. F. Syverson, D. M. Goldschlag, and M. G. Reed, “Anonymous connections and onion routing”. In Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, pp. 44–54, 1997.

[19] M. Reiter and A. Rubin. “Crowds: Anonymity for Web Transaction”. ACM Transactions on Information and System Security, volume 1, issue 1, pp. 66–92, 1998.

[20] A. Beimel and S. Dolev, “Buses for Anonymous Message Delivery”. Journal of Cryptology, volume 16, pp 25–39, 2003.

[21] L. Ahn, A. Bortz, and N. Hopper, “K-anonymous message transmission”. In Proceedings of the 10th ACM conference on Computer and Communications Security, Washington D.C., USA, pp. 122–130, 2003.

Back to the Future: Evaluation Model for Wearables Based On the Past Experience

Marta Piekarska and Shinjo Park and Altaf Shaik
Security in Telecommunications
Technische Universität Berlin
Berlin, Germany
Email: marta OR shinjo OR altaf@sec.t-labs.tu-berlin.de

***Abstract*—Today every user has a plethora of devices to choose from, depending on the task. In addition to omnipresent laptops, smartphones and tablets, we have recently seen an expansion of a new type: the wearables. Wearable devices vary from fitness trackers, through watches and glasses, all the way to medical-grade equipment. This Systematization of Knowledge paper investigates the historical shift in the security and privacy considerations when smartphones started replacing laptops, and tries to predict how the change will look like this time. We examine the categories of attacks on laptops and mobile devices and analyze how those will work on wearables. We also recognize the additional threat layers when these elements are combined into Internet of Things. Finally, we propose mitigations and potential defenses to some of the biggest challenges. In summary this paper contributes to the field by a thorough systematization of knowledge of the attack vectors on various devices and proposes a method of predicting the security threats to new device types.**

***Index Terms*—privacy, internet of things, wearables, systematization of knowledge**

I. Introduction

Personally Identifiable Information is a concept describing linking of attributes (has cancer or is in a certain location) to a particular person. It ranges from strictly private data like phone number or address, through common locations all the way to browser fingerprinting [1].

The market of wearable technology is predicted to rise to over $37B by the end of 2020 [2]. It is not yet well understood what will be the consequences of such expansion on privacy and security. One is sure: nowadays computer security impacts everyone, even if they don't use what they think of as a ”computer” [3]. In fact, any modern computer is a system far too complex for any individual to grasp it as a whole. The problem of securing every element of the stack gets additionally complicated when we grow it by connecting several devices into Internet of Things. The number of attack vectors does not simply become a sum of attacks on each device included.

With our work we contribute by:

1) **Systematization of Knowledge**
2) **Possible Attack Vectors for Wearables**
3) **Security of Internet of Things**
4) **Countermeasures and defenses** to the identified problems

The rest of the paper is organized as follows. The next section talks about the history: what were the threats that were common to laptops and smartphones, and what were the problems previously unknown that emerged with the popularization of the smartphones. Section II describes the model that we built to evaluate any new device. We then apply this model to present the evaluation of wearables in Section III. Next, in Section IV we spent some time to point out the elements very specific to the nature of Internet of Things. Finally, in Section V we present some of the suggested defenses and mitigations, and conclude in Section VI.

II. Building a Model

We have found very few approaches that try to systematize the evaluation of the devices. Among them there is [4] where the authors tried to predict the future of mobile phones by analyzing the models, algorithms, applications and middleware. In their followup work from 2014 [5], they note however, that the approach did not prove to be useful, and they failed to predict certain developments. Another notable paper was written by Delac et al [6], in which authors summarize the mobile security threats. It is a good but post-factum analysis, and their model does not scale to other device types.

We assume that the technology moves in an upward spiral manner and every new device is build on top of the previous ones, which makes the assessment simpler. Moreover, we believe we can build a universal security stack where each layer is protected by the previous ones. Lastly we think a complete analysis can be performed by naming the assets, identifying the threats, looking at historical vulnerabilities and attacks, and defining the risks.

Security assessment can be seen as a cycle of 6 steps. Initially, we define the assets a device can hold, next we try to find the threats, identify the vulnerabilities, and ways to exploit them, finally predicting the risks connected to those we can focus on designing countermeasures and implementing defenses. However, looking just at the big picture might not be enough for a complex system. That is why we define layers of security stack that need to be inspected. On the bottom there is the Network Infrastructure - everything that allows a device to stay connected. Next comes the hardware - physical elements that comprise a device, like sensors, memory etc. Together with it we need to consider the drivers that allow

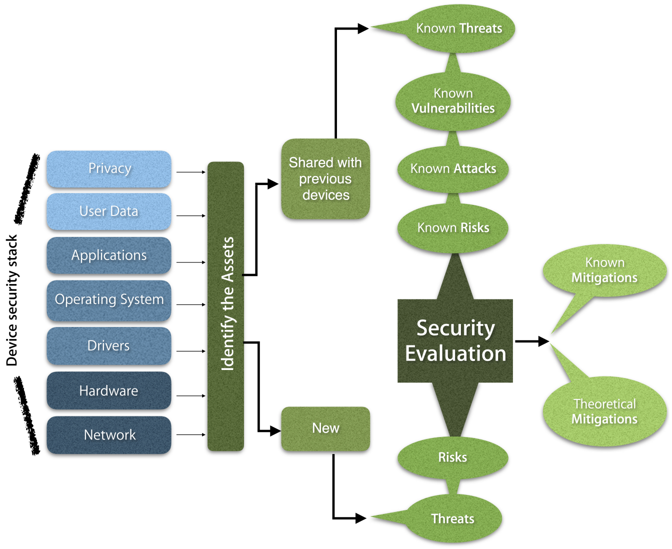


Fig. 1. Model for security evaluation of a new device.

for access and manipulation of the device. The layer above that is the Operating System(OS) that governs the behavior of the device, and manages access control to the file systems. On top of the OS, in most cases, sit the applications - some devices, like the fitness trackers will not allow for third party applications, but still there is a software installed in addition to the OS. Finally we come to the user data which is all the information that an owner of the device generates, everything that can be considered PII. We put privacy on top of the stack, as protecting it mostly means protecting from leakage of user data. The model we build based on the above assumptions is presented in Figure 1.

III. Security Evaluation of Wearables

Having a model and some hints on what are the differences and commonalities between security challenges on laptops and mobile devices, we now move to evaluation of the wearables.

A. Assets

We consider four types of wearable devices: fitness trackers, smartwatches, headmounted devices and medical devices(IMDs).

Each layer of the security stack has many assets connected to it. In case of mobile devices and smartwatches we first have the network: the contents of communication that goes over the channels and the infrastructure. Next, there is the hardware: sensors the device has. The more sensors there are, the more possibilities of attacks.

On the software side, we start with the drivers: ensuring the integrity of the binary files so that the attacker cannot manipulate the hardware. In the Operating System we have its integrity, access to the memory, availability. Next, come the applications. What is protected is again thier integrity and availability of the services.

We then come to the third big part - the user data and privacy. In case of fitness trackers data includes fitness level that comes from monitoring the heart rate – the pulse, estimation of calories burned etc, location over time, sleep patterns and user-input data like their age, weight, height and so on. In terms of smartwatches in addition to the above we have much more elaborate health data that can be tracked either with the watch itself or by connecting other monitors to it. These include e.g. nutrition facts, reproductive health, blood pressure, temperature and so on. Additional data contain things we normally think of in terms of mobile devices: recordings and photos, contacts, passwords, list of applications, emails and messages and so on. Lastly, protecting the integrity and confidentiality of the data stored.

B. Threats

Wearables have the same set of sensors, are connected, quite powerful, very personal. Depending on the category, the threat models will be slightly different: fitness trackers and medical devices are less powerful, thus will not be used for heavy computations, while smartwatches and glasses are almost identical in construction to mobile devices and will be exposed to threats.

On the network level the threats are similar, as the assets are also fairly identical: the Golden Graal is to be able to intercept and possibly modify data that come from and to the wearable. The impact and incentive, however, is higher as the data is more valuable. Most of the wearables use the same connectivity methods as mobile devices: Bluetooth, ANT radio, cellular data and Wi-Fi. Some devices, use proprietary protocols or advance of software-defined radio (SDR) enabled decoding of proprietary wireless communication standards. [7]. The threats include: stealing the contents of communication, gaining access to the elements of a network (eg., Wi-Fi hotspots, Base transceiver station (BTS) etc.), modifying the contents of communication and altering the message path (forwarding the message to unauthorized person).

Most of the wearables, are still dependent on a ”bigger brother” - be it a smartphone, a laptop, or a dedicated terminal - to process data and perform heavier computations. Thus another threat is intercepting or modifying that communication. That requires compromising the OS or gaining access to the hardware. As wearable devices almost always have a full OS installed, in these terms, again the threats popular in mobile devices will also apply to them. Thus, poor user authentication due to the form factor and lack of secure key storage can be seen as big challanges.

Finally, threats to privacy on wearables are more significant. Data is collected unconciously and becones very valuble. Its improper protection of the data may also lead to leakages that can be dangerous (revealing information about location), embarrassing (search history), or cause financial losses (access to payment information). Moreover the stealth capturing of scenes can be abused by either the attacker or the owner spying on the surrounding. Until today many companies have ot yet included Wearables into their Mobile Device Management policies.

Final threat to privacy is based on the correlating data. What happens if the increased heart rate is combined with information that the user is in a hotel during work hours? What is in addition to it we can also find the sounds in the room? Can we then accuse them of adultery?

Due to the form factor of the screens the way we inteact with wearables has changed compared to other devices. Voice recognition became more popular way of navigating these devices which means more data transmitted and stored over potentaily insecure channel. Lack of proper displays also impairs the way we can inform users about the privacy policies and warnings, which means poor transparency. Wearable devices are powerful, have access to a lot of information about their owners, yet present no transparency of what tasks are being executed.

Laptops gather information about our activity, mostly things we download, history of usage. Smartphones have the ability to record elements like our position, movement, things that happen around us - through camera applications. Wearables go further. More than any others, these devices are able to collect more precise data over time - gathering a detailed description of the owner's life. They can also be better instrumented to understand the context in which user is. Without good diversification it is easy to gain access to information about user's whole life just by attacking this singe element.

Wearables as a new category of devices are not yet subject to any standardization procedures. We still lack policies that would describe how to deal with the authentication problems - what are good ways to implement secure storage on devices, how to manage the Personally Identifiable Information(PII), and most importantly - what to do with very sensitive data, like health results. The threat is that without such standards every manufacturer will implement their own, possibly faulty, mechanisms.

C. Vulnerabilities and Attacks

One of the earliest attack on fitness tracker is done by Rahman et. al [8] using Fitbit. It presents attack on spoofing device sensor, eavesdropping and injecting data between base and web services.

1) Smart Watches: A good overview is provided by HP Fortify and the Internet of Things report [9]. They have evaluated top 10 smartwatches and found that 70% of the firmwares is sent through unencrytpted channels, 30% of the devices were vulnerable to Account Harvesting, allowing attackers to guess login credentials and gain access to user account, and as much as 90% of communication(!) could be easily intercepted.

One of the earliest attacks on MDs is presented by Halperin et. al [7] in 2008. This work covers security of externally controllable implanted pacemaker. Kune et. al [10] presented EMI injection attack on medical sensors inside pacemaker, which could trigger unintended operation of medical devices.

In October 2011 Barnaby Jack managed to override the insulin pump's radio control and its vibrating alert safety feature, enabling to dose a an unaware patient with a lethal amount of insulin [11]. Li et. al [12] also presented an attack on insulin pump with similar result.

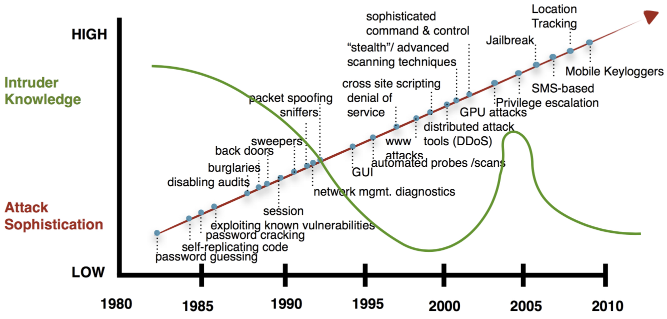


Fig. 2. Attack Sophistication vs. Intruder Technical Knowledge.

The conclusion can be drawn that a significant problem with medical wearables comes from the fact that we are still in the phase of patching together existing devices with embedded computers rather than designing them from the scratch. We have little to no "Security by Design" approach, which is crucial as we are speaking of things that when exploited, more than any others, can threaten human lives.

Wearables mostly inherit Operating Systems from smartphones. That means that whatever could be exploited on one can also be done on the other. Thankfully manufacturers tend to improve their systems and patch the bugs which means that old problems cannot be revisited. However we have already seen report that Google Glass runs Android 4.0.4, which is subject to the adb restore race condition [13].

D. Risks

In his report from 2002, Lipson, presented how the sophistication of attacks developed while the intruders technical knowledge dropped over time [14]. Figure 2 is an extension of the original one with attacks that have become biggest risks to smartphones, like rootkits or location tracking. As can be seen, we believe that there was a brief spike in the requirement in the knowledge of an intruder when a new device type was introduced - it was no longer as obvious as before how to attack it. But we quickly got back to repackaging everything into simple tools and today, it is enough to go on a website that will give you those information, or download a simple package to jailbreak your iPhone.

The risks are directly proportional to what the attacker can gain. In the era of laptops the goal was gaining access to computing power. Distributed attacks were created so that viruses could spread in millions of copies and allow intruders to create a network of computers working to their advantage. Today even the attacker model changed: one is Malfoy, who owns a device and wants to root it. He becomes a hostile actor towards his own device. Second is Mark, who tries to steal data off other devices. And Mark in the world of smartphones will not seek computing power. It is too cheap to buy otherwise. He will want to gain access to PII, most probably to later sell it to advertising companies or governments. Today it is the information that brings money and is most valuable.

IV. When it all comes together: IoT

Internet of Things(IoT) is not just a combination of various devices connected with each other. The attack surface is not calculated by a simple addition of all attacks known to each of the elements of IoT but a multiplication.

A. Assets

For the purpose of this paper we will focus on a ”single user IoT”: what happens when we connect wearables with smartphones and laptops. On top of what each of those ”things” brings to the table additional assets include:

- communication between devices,
- ability to control one through the others,
- ability access data over another device,
- pervasiveness - even if one device is not there, another will be,
- permissions given to each device.

On the last point: there is no clear way how to negotiate and see sharing data between the devices. It is not necessarily the case that user will agree to tracking on every element of IoT - if so, how should that communicate to the other ”things”?

B. Threats

The problem with IoT is that each of its elements is different, yet a security solution must cover it all. The design is influenced by the threat model, device architecture, protocols and interfaces required and power and performance targets. In addition to protecting each element separately, a mechanism of ensuring trust between them has to be deployed. Now, the CIA – Confidentiality, Integrity and Availability has a second level. Each ”thing” has to have an identity that can be proven to other devices, it has to act in a predictable way that cannot be altered by an attacker to change the behaviour of the whole system. What follows is that the communication channels between the elements have to be protected from unauthorized access, as well as the data on the devices. Most importantly, it is crucial to ensure a certain separation – so that failure of one ”thing” does not compromise the whole system. The devices that comprise IoT are often produced by various vendors and need to communicate, which may create various problems with the protocols: they need to be well examined and understood.

C. Vulnerabilities and Attacks

Security of IoT is a big problem. 80 percent of Amazon’s top 25 best-selling SOHO wireless router models have security vulnerabilities [15]. What is more scary, the same report states that almost one third of IT professionals and 46% of employees do not change the default administrator password on their wireless routers. A big part of IoT threat is that whatever happens the impact will be bigger. There are more devices, more computing power, more data, thus more incentives and more vulnerabilities.

IoT devices are operating in non-traditional area of network, like personal area network (PAN), body area network (BAN) or controller area network (CAN). Like Ubertooth for Bluetooth, KillerBee can decode ZigBee and IEEE 802.15.4 packets. [16] ZigBee and/or IEEE 802.15.4 is used in home appliances, thermostats, manufacturing systems, medical devices, retail, transportation, etc. KillerBee provides tools to capture and decode 802.15.4 signals, with custom firmware on AVR RZ Raven USB stick as radio device. Choi et. al [17] presented reverse engineering IEEE 802.15.4 based home and transportation appliance using KillerBee.

IoT devices communicating with BLE or other insecure channel share the communication privacy and identity problems [3], [18]. Unlike wearables, IoT devices are designed with infrequent human interaction and longer continuous operation in mind. As a result, security incident reported by IoT devices might not be handled in timely manner, and software patching for security problem could not be possible in some cases where parts are discontinued or a manufacturer has been closed.

V. Defenses and Mitigations

We will now discuss technical countermeasuers and design considerations of wearable devices which allow the users to monitor and control the exposure of their private data from the wearable device.

A. Authentication and encryption techniques

Although the main focus of existing literature is on securing MDs [19], we believe that the same defence measures can be applied to other types of wearable devices. One of the first concepts proposed was symmetric-key based authentication methods for distributed access control in wearables [20]. By pre-distributing the keys, the device and any authorized body can easily generate pairwise keys to perform authentication. However, Symmetric Key Cryptography (SKC) based methods suffer from numerous disadvantages [21].

There are SKC-based techniques that do not depend on pre-distributed keys and require additional hardware devices [22]. This out of band secure channels inlude USB connections [23], infrared [24], visual [25], audio but mean adding extra hardware. This requirement is unrealistic and is against the global trend of device miniaturization.

In Identity Based Encryption (IBE) technique where no prior key distribution is necessary between the users and devicescite [26]. On the other hand, traditional IBE techniques demand heavy computation and are not appropriate for body area networks. To solve this problem authors of [27] provide a lightweight IBE-based access control mechanism built using elliptical curve cryptography (ECC). Its main limitation is that once a certain number of secret keys are leaked, the master key can be compromised. Besides IBE, Attribute Based Encryption (ABE) is also studied in the literature. For example, ciphertext policy ABE was introduced in [28] to allow role-based access control on encrypted data in WBAN’s.

Authentication with non-cryptographic methods such as proximity based, biometric based and channel based methods are also studied in the literature. By extending the Diffie-Hellman (DH) key exchange protocol the authors in [29] could develop authentication mechanism for co-located devices. Ensemble technique [29] and co-location based pairing scheme [30] also propose proximity based authentication scheme. Ramussen et al. [31] use ultrasonic sound signals to compute the distance between the programmer and IMD. Capkun et al. [32] proposed integrity code which protects the integrity of the messages sent over insecure wireless channel. Gollkota et al. [33] proposed tamper-evident pairing. It assumes infeasibility of signal cancellation, and exploits unidirectional error detection codes to provide message tamper-evidence.

The use of physiological signals (biometric data) for securing wireless medical devices was first introduced in 2003 [34], and later adopted for electro-cardiogram(ECG) and photo-plethysmogram (PPG) signals by Poon et al. in 2006 [35]. Further, in [36], inter-pulse intervals (IPIs) and heartbeats are potential source for generating secret keys. Besides that, a more robust usage of IPIs with measurement noise for authentication is presented in [37]. However, encryption based on ECG signals is more prominent in the literature [38], [39], because of its higher randomness as compared to other physiological signals (PVs)such as heart rate, glucose level in blood, blood pressure and temperature along with the preceding ones.

In general, due to their unique, random and time-sensitive nature, physiological information can serve as a reliable source for authentication and secret key derivation among the wearable devices. Nevertheless the major drawback is that physiological information is usually accompanied with high amounts of noise and variability. Hence it is difficult to guarantee consistent physiological measurements with same accuracy for sensors located on different positions on human body. Moreover, all physiological parameters do not have the same level of entropy for key generation.

B. Design Considerations

Hitachi's Business Microscope identity badge, which contains embedded infrared sensors, an accelerometer and a microphone sensor, purports to capture the interaction patterns in the workplace but also the quality of employee collaboration [40]. Monitoring of our emotions, health status and the quality of our human interactions strikes at the very core of our most intimate selves. The interaction medium with the wearable device also has an impact on the user's privacy. The users capability to modify, perhaps switching the input mode from audio to text would be a possible design modification to enhance privacy.

User privacy is one aspect but the privacy of others around the user is another. With wearable devices, that are seamlessly embodied into undistinguished objects, such as shirt buttons, eyeglass frames, watches it is quite effortless to gather information about others without their awareness [41]. Similarly, users have privacy concerns about location information, primarily because wrist-mounted devices are able to track their position and immediately publish it online in social media applications to a network of contacts. To combat this issue users must be able to choose their desired level of privacy.

Roesner et al. identified potential security issues with wearable devices and explored the problems these devices create in terms of law and policy [42]. Further, researchers have studied several methods to protect privacy in an IoT scenario. Examples of such works include frameworks to design for protocols for communication, privacy focused designs, protocols for anonymous communication, evaluation metrics for privacy and its models. At the same time, the legal frameworks need to adapt to the use of wearables, as they put new requirements on the protection of personal integrity and privacy as well as information security.

It is essential to abide by certain design principles enumerated below, for protecting privacy in the wearable computing environment, as the characteristics of today's wearables evolve in tandem with the Internet of Things.

- transparent authentication and security mechanisms and device functionalities
- dynamically calibrated privacy rules that provide tight control of what the device does
- user controlled network connection and disconnection
- privilege escalation on the device

Finally, practical implementation of security measures in wearable devices depends on several factors. There is no single method that suits all situations. One needs to collectively consider the application security requirements, system security requirements, hardware/software/physical/power restrictions and the possible tradeoffs among them.

VI. CONCLUSIONS

In this paper, we built a general model to evaluate any new device on the market based on the past experiences rather than from the scratch. We observed how did the attacks change when smartphones took over the market. We applied the model to predict the future problems that we will see in the wearables. We also presented what we see as the biggest challenges that Internet of Things will face - the multiplication rather than addition of attack vectors. Finally, we discussed what could be the possible defense mechanisms that we should build prior to the attacks.

Among various security measures, authentication and encryption are the crucial steps in building secure communications with the wearables. Additionally we need to develop dynamically calibrated privacy rules to meet individual's privacy needs and expectations, integrate simple design features so that the wearable device can reflect personal privacy preferences, and call on organizations to enhance their privacy policies with dynamic and interactive data maps and infographics to show relationships in the wearable computing device ecosystem. Finally, it is important to touch on the question of transparency. While security is a problem that can be boiled to meeting a certain standard, sometimes the best we can do in terms of privacy is being clear about what and when happens on the device. We are lacking mechanisms that inform users that their data is being collected and uploaded in the real time. We see that as the next challenge to the academia.

REFERENCES

[1] E. McCallister, T. Grance, and K. A. Scarfone, "Sp 800-122. guide to protecting the confidentiality of personally identifiable information (pii)," Tech. Rep., 2010.

[2] Research and Markets, "Global smart wearables market forecast and opportunities, 2020," Tech. Rep., 2015. [Online]. Available: http://www.researchandmarkets.com/research/j7fhxw/global_smart

[3] F. Stajano, *Security for Ubiquitous Computing*, 2002. [Online]. Available: http://www.cl.cam.ac.uk/∼fms27/secubicomp/

[4] G.-C. Roman, G. P. Picco, and A. L. Murphy, "Software engineering for mobility: A roadmap," ser. ICSE '00. [Online]. Available: http://doi.acm.org/10.1145/336512.336567

[5] G. P. Picco, C. Julien, A. L. Murphy, M. Musolesi, and G.-C. Roman, "Software engineering for mobility: Reflecting on the past, peering into the future," ser. FOSE 2014. [Online]. Available: http://doi.acm.org/10.1145/2593882.2593884

[6] G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in *MIPRO, 2011 Proceedings of the 34th International Convention*.

[7] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," *Proceedings of IEEE Symposium on Security and Privacy*, 2008.

[8] M. Rahman, B. Carbunar, and M. Banik, "Fit and vulnerable: Attacks and defenses for a health monitoring device," *Privacy Enhancing Technologies Symposium*, 2013. [Online]. Available: http://arxiv.org/abs/1304.5672

[9] C. Smith and D. Miessler, "Internet of things security study: Smartwatches," Tech. Rep., 2015. [Online]. Available: http://go.saas.hp.com/fod/internet-of-things

[10] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," *Proceedings of IEEE Symposium on Security and Privacy*, 2013.

[11] D. Goodin, "Insulin pump hack delivers fatal dosage over the air," *The Register*, 27 Oct 2011. [Online]. Available: http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

[12] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2011*, 2011.

[13] [Online]. Available: https://twitter.com/saurik/status/327857009754001408

[14] H. F. Lipson, H. F. Lipson, P. D, and P. D, "Tracking and tracing cyber-attacks: Technical challenges and global policy," 2002.

[15] T. Vulnerability and E. R. Team, "Soho wireless router (in)security," 2014. [Online]. Available: http://www.tripwire.com/register/soho-wireless-router-insecurity/showMeta/2/

[16] J. Wright, "KillerBee: Practical ZigBee Exploitation Framework," 2009.

[17] K. Choi, Y. Son, J. Lee, S. Kim, and Y. Kim, "Frying PAN : Dissecting Customized Protocol for Personal Area Network?" *Proceedings of the 16th International Workshop on Information Security Applications*, 2015.

[18] D. Kozlov, J. Veijalainen, and Y. Ali, "Security and Privacy Threats in IoT Architectures," *International Conference on Body Area Networks*, 2012.

[19] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," *Proceedings of IEEE Symposium on Security and Privacy*, 2014.

[20] M. Mana, M. Feham, and B. A. Bensaber, "A light weight protocol to provide location privacy in wireless body area networks." [Online]. Available: http://arxiv.org/abs/1103.3308

[21] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *Wireless Commun.*, 2010. [Online]. Available: http://dx.doi.org/10.1109/MWC.2010.5416350

[22] M. Li, S. Yu, W. Lou, and K. Ren, "Group device pairing based secure sensor association and key management for body area networks," ser. INFOCOM'10. [Online]. Available: http://dl.acm.org/citation.cfm?id=1833515.1833857

[23] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks."

[24] D. B. Smetters, D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks," 2002.

[25] C.-H. O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J. M. McCune, A. Studer, A. Perrig, B.-Y. Yang, and T.-C. Wu, "Gangs: Gather, authenticate 'n group securely," ser. MobiCom '08. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409957

[26] C. Rong and H. Cheng, "Authenticated health monitoring scheme for wireless body sensor networks," ser. BodyNets '12. [Online]. Available: http://dl.acm.org/citation.cfm?id=2442691.2442700

[27] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Ibe-lite: A lightweight identity-based cryptography for body sensor networks," *Trans. Info. Tech. Biomed.*, 2009. [Online]. Available: http://dx.doi.org/10.1109/TITB.2009.2033055

[28] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," ser. SP '07. [Online]. Available: http://dx.doi.org/10.1109/SP.2007.11

[29] A. Varshavsky, A. Scannell, A. LaMarca, and E. De Lara, "Amigo: Proximity-based authentication of mobile devices," ser. UbiComp '07. [Online]. Available: http://dl.acm.org/citation.cfm?id=1771592.1771607

[30] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: Proximity-based secure pairing using ambient wireless signals," ser. MobiSys '11. [Online]. Available: http://doi.acm.org/10.1145/1999995.2000016

[31] K. B. Rasmussen and S. Čapkun, "Realization of rf distance bounding," ser. USENIX Security'10. [Online]. Available: http://dl.acm.org/citation.cfm?id=1929820.1929854

[32] S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," *Dependable and Secure Computing, IEEE Transactions on*, 2008.

[33] S. Gollakota, N. Ahmed, N. Zeldovich, and D. Katabi, "Secure in-band wireless pairing," in *In USENIXSecurity Sym.,2011*.

[34] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, "Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Parallel Processing Workshops, 2003*, 2003.

[35] C. C. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *Comm. Mag.*, 2006. [Online]. Available: http://dx.doi.org/10.1109/MCOM.2006.1632652

[36] S.-D. Bao, C. C. Poon, Y.-T. Zhang, and L.-F. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *Trans. Info. Tech. Biomed.*, 2008. [Online]. Available: http://dx.doi.org/10.1109/TITB.2008.926434

[37] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (h2h): authentication for implanted medical devices," ser. CCS '13. [Online]. Available: http://doi.acm.org/10.1145/2508859.2516658

[38] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "Pska: Usable and secure key agreement scheme for body area networks," *Information Technology in Biomedicine, IEEE Transactions on*, 2010.

[39] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, "Imdguard: Securing implantable medical devices with the external wearable guardian," in *INFOCOM, 2011 Proceedings IEEE*.

[40] R. G. of the Office of the Privacy Commissioner of Canada, "Wearable computing: Challenges and opportunities for privacy protection," 2014.

[41] K. Krombholz, A. Dabrowski, M. Smith, and E. Weippl, "Ok glass, leave me alone: Towards a systematization of privacy enhancing technologies for wearable computing," in *1st Workshop on Wearable Security and Privacy*, 2015.

[42] F. Roesner, T. Denning, B. C. Newell, T. Kohno, and R. Calo, "Augmented reality: Hard problems of law and policy," ser. UbiComp '14 Adjunct. [Online]. Available: http://doi.acm.org/10.1145/2638728.2641709

A Code Offloading Framework for Mobile Cloud Computing: ICEMobile

Emre Çalışır
Computer Engineering Department
Galatasaray University
Istanbul, Turkey
e-mail: emrecalisir@gmail.com

Gülfem Işıklar Alptekin
Computer Engineering Department
Galatasaray University
Istanbul, Turkey
e-mail: gisiklar@gsu.edu.tr

B. Atay Özgövde
Computer Engineering Department
Galatasaray University
Istanbul, Turkey
e-mail: aozgovde@gsu.edu.tr

Abstract— **Smartphones have become a crucial part of our life with their high performance data processing features and ability to access information from anywhere at any time. However, they tend to become inadequate to meet computation intensive operations with their limited battery life and processing capabilities. Mobile cloud computing may be a solution, but Wide Area Network (WAN) latencies and unstable response times of cloud services negatively affect user experiences. In this paper, the cloudlet approach, which offers the cloud services with Local Area Network (LAN) bandwidth, is presented as a possible solution to this problem. A framework, called ICEMobile, is introduced that brings the computation offloading capability to mobile applications. The aim of the ICEMobile framework is to direct application developers in determining which methods need to be offloaded in order to save energy during the mobile execution. The applicability and efficiency of the framework and related optimization model are shown via real life scenarios. The test results reveal that it is possible to save energy up to 98% on the mobile device by using the proposed framework.**

Keywords—mobile cloud computing; cloudlet; code offloading; energy efficiency

I. INTRODUCTION

The evolution of digital world is correlated with the fulfillment of people's expectations that can be summarized as accessing technology from anywhere and anytime, called as ubiquitous computing. It is the method of enhancing computer usage by making many computers available throughout the physical environment, but making them effectively invisible to the user [1]. With the increasing mobility of people and the rise of social media, people’s behaviors are changing towards using small and portable personal computers to benefit from vast resources through Internet. On the other hand, the need for intense computation is ever increasing. However, current smartphones are unable to respond these needs because of their limited battery life and CPU power. At this point, cloud computing comes into the scene since it enables retrieving on-demand services from a shared pool of configurable computing resources [2]. Combining ubiquitous computing, mobile computing and cloud computing, a new model, called Mobile Cloud Computing, is developed to bring cloud computing services into the edge to extend resource-rich services on the mobile devices [1].

A cloudlet is a small-scale cloud-like infrastructure, which is located in one hop distance to the mobile user and connected with a high network speed. Cloudlets are fully dedicated to the mobile devices with the aim of executing their resource intensive but latency-sensitive tasks [3]. A mobile device that is connected to a cloudlet benefits from much powerful computing capabilities and unlimited power. These benefits are also valid for distant cloud-based computation; however, in that case it may occur serious time losses due to ambiguous service response times of the cloud and WAN latencies. Therefore, offloading to a distant cloud is not always a solution. The computation or code offloading paradigm means transferring complex tasks to more powerful environments.

In this paper, we develop a framework having code offloading capability and examine three use cases containing computation-intensive operations. The framework involves a decision making engine that analyzes efficiency of the given application. Doing so, we generate the call graph of the program and analyze in detail the time cost of each node and edge. We then test this mechanism with an Android application and a Java based web server, which are connected with the RESTful web services during the execution of three computation-intensive use cases.

The remaining part of the paper is structured as follows: Section 2 presents related works in literature. Section 3 introduces the proposed ICEMobile architecture with its optimization model. In Section 4, experiments and results are given. Finally, the last section presents concluding remarks driven from the test results.

II. LITERATURE REVIEW

The studies in literature that consider the idea of moving the cloud closer have started with the ‘cloudlet’ concept of Satyanarayanan et al. [3]. With the impact of this novel approach, it has recently become a hot topic in mobile cloud computing related research. In this cloudlet model, the cloudlets are at one hop distant to the mobile device, having high bandwidth wireless access. They may be located in coffees, airports like wireless hotspots to deliver instant services to the mobile clients. The proposed computation offloading techniques in [3] are virtual machine (VM) migration and dynamic VM synthesis. In VM migration, the entire snapshot of the mobile device is transferred to the cloudlet, while in the second technique, there is a dynamic VM synthesis to reduce the size of the VM snapshot by receiving the delta with the previous VM state. The dynamic VM synthesis technique provides offloading capability for each mobile device, since it transfers the VM of the mobile device rather than platform specific objects. On the other hand, it contains many problems especially related with user experience and lack of a decision engine.

ISBN: 978-1-61208-503-6

Another research, entitled as MAUI, targets to offload only the computation intensive parts of the mobile application with method-level offloading based on the .NET framework [4]. In this research, a system is proposed, which is capable of making the decision of whether offloading will save energy for each offloadable part of the application. The proposed method-level offloading type is a more fine-grained approach than the VM migration or dynamic VM synthesis. In addition to reducing size of the transferred objects, MAUI also provides an intelligent mechanism targeting to reduce the energy consumption on the mobile device by optimally deciding to offload subject to device and server capabilities and network conditions. However, some of the processes in MAUI framework prevent creating dynamic code offloading environments. The first issue is having the necessity of modification on the application since it seems as a disadvantage comparing to [3]. Secondly, there is not any mechanism for automatically identifying the computation intensive parts of the application.

Another research entitled as CloneCloud, focuses on the application partitioning and thread-level offloading [5]. The VM migration mechanism is used in the background of this study by offloading execution blocks of applications from smartphones to their mirror image running on the server. This framework works as a middleware in Android OS, on the top of Dalvik VM. An advantage of the CloneCloud is that it does not require developers' modification.

In addition to the previous studies, a research, called Cuckoo, focuses creating a dynamic offloading decision making tool in runtime in Android OS installed smartphones [6]. It presents a system to offload mobile device applications onto a cloud using a Java stub/proxy model. Cuckoo can be offloaded onto any resource that runs the Java VM. In order to use Cuckoo, the applications need to be re-written such that the application supports remote execution as well as local execution. Moreover, it does not contain any optimization when deciding to offload; instead it always offloads when it connects to the cloud. In a recent related work [1], Zhou et al. propose a context-aware offloading decision algorithm that works on a mobile cloud computing offloading system with multiple cloud resources. Their algorithm takes into account the context changes to select the wireless medium to utilize.

The offloading granularity and optimization mechanism of ICEMobile framework are similar to MAUI's model. However, our approach is typical client/server architecture rather than being a middleware of the device operating system.

III. ICEMOBILE ARCHITECTURE

The focus of our proposed framework ICEMobile is to minimize the energy consumption of the mobile device when computation-intensive functions need to be executed. Doing so, it transfers the resource-intensive code partitions of mobile application to the cloudlet for remote execution. The main purpose is to extend battery life of the mobile device. The energy consumption of the cloudlet is not the concern in this paper, since it is assumed to be continuously fed from the energy sources. The ICEMobile framework architecture is depicted in Fig. 1. It involves Remote Method Invocation (RMI) framework both in the mobile platform and in the cloudlet. In case of cloud-based offloading, it is possible to integrate this framework into the cloud configuration. The advantage of using the nearby cloud in LAN is that it provides higher bandwidth compared to the one in WAN. Besides, it does not require having Internet connection since the cloudlet is ready to satisfy all client needs. In case of need to extra resources, the distant cloud services may be used, but in that case the user experience may be decreased, especially when real-time computation-intensive operations are executed. The essential part of the ICEMobile offloading framework is in the server side, where there is not any limitation on the operating system with the help of JVM technology. The environmental profiling and program analyzing efforts together with the optimization component in the server side enable optimal decision making for offloading. In this architecture, the Profiler and the Analyzer are not executable programs. The developer manually operates them and their outputs are transmitted to Optimization Solver as input. This process is realized automatically in [5]. In addition to these components, the same offloadable methods of the mobile application are also present on the cloudlet to be executed when necessary.

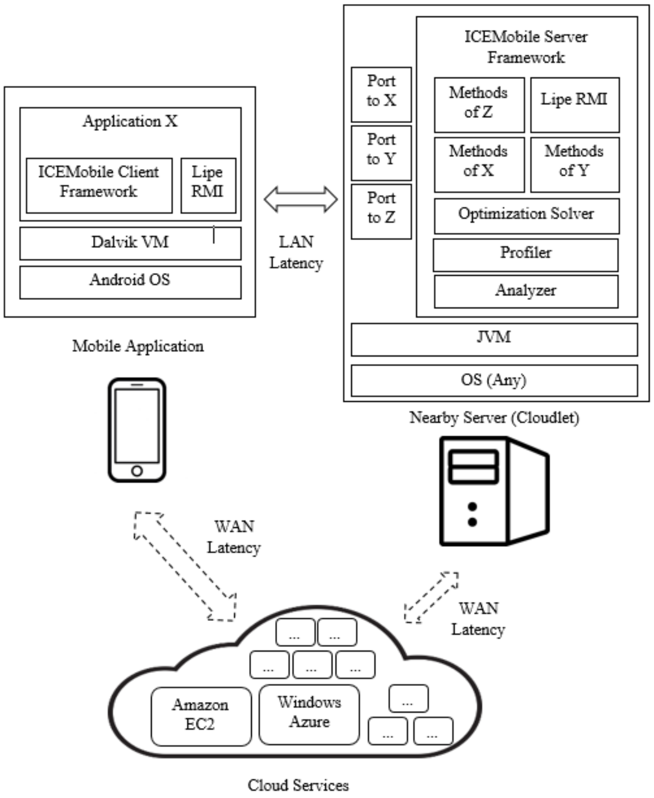


Figure 1. ICEMobile System Architecture

In the client side, any mobile device can benefit from the ICEMobile task offloading mechanism. For mobile devices with higher computational capabilities, the need for offloading tends to decrease. In order to promote offloading, the application code needs to be modified with the ICEMobile client framework codes. In the server side, a port is specifically reserved for each client. In order to initiate the server, the following two steps are proceeded:

i. A *CallHandler* is identified. The interface file that keeps the method signatures and the class file that contains the client methods are globally registered to *CallHandler*.

ii. *CallHandler* is bounded by the available port to start listening the environment and respond to the incoming requests.

A. Making the Optimal Offloading Decision

The optimization solver in the ICEMobile framework aims at determining which portions of the application code are better to be offloaded to the remote server in order to use resources more effectively. The decision making procedure is based on the model proposed in [4]. The advantage of offloading in method-level granularity is the ability to transfer only the computation-intensive parts of the application, rather than transferring the full VM snapshot, as in [3]. In the first step of the ICEMobile optimization process, the application is analyzed via its call graph. In order to extract the call graph, static or dynamic analyzers can be used. Next, each node and edge in the call graph is attached with a time and energy cost. The measurements are generated for each of the following three cases:

- Perform all methods on the mobile device and measure the time and energy cost,
- Perform all offloadable methods on the cloudlet and measure the time cost,
- Offload all offloadable methods and measure the time and energy cost.

The energy cost is measured using the Android application called PowerTutor. At the end of the optimization process, the nodes that are better to be offloaded is determined. The offloading variable in the objective function is a binary one that has two values: 0 for not offloading, and 1 for offloading. The given maximization problem is solved by *lpsolve* solver of the R language.

For a given graph *G*=(*N*, *E*), *N* represents *node* and *E* represents *edge*. Each node $n \in N$ represents a method and edge *e*=(*m*, *n*) represents an invocation of method *n* from *m*. We annotated each node $n \in N$ with the energy it takes to execute the method locally E_n^l. The energy consumption of the cloudlet is not considered. The time that a node takes to execute the method locally is shown by T_n^l, and the time that a node takes to execute the method remotely is specified by T_n^r. Each edge is annotated as *e*=(*m*, *n*). The time it takes to transfer the necessary program state is given by $B_{m,n}$ when *m* calls *n* and the energy cost of transferring that state is annotated as $C_{m,n}$. The binary parameter r_n indicates whether the node *n* is offloadable or not.

The 0-1 integer programming function of ICEMobile is shown in the equations (1), (2) and (3) [4]. The objective is to maximize the energy savings in the mobile device (1). The optimization solver determines the offloading variables (I_n) that is the indicator variable of offloading decision for each node. As a result of the optimization, if I_n is equal to 0, it means that the method will not be offloaded and if I_n is equal to 1, the method will be offloaded and it will result in saving energy.

$$\max \sum_{n \in N} I_n . E_n^l - \sum_{(m,n) \in E} \left| I_m - I_n \right| . C_{m,n} \tag{1}$$

$$s.t. \sum_{n \in N} ((1 - I_n) T_n^l) + (\mathrm{I}_n . T_n^r) + \sum_{(m,n) \in E} \left| I_m - I_n \right| B_{m,n} \leq L \tag{2}$$

$$I_n \leq r_n, \forall n \in N \tag{3}$$

The ICEMobile client framework contains the RMI interfaces presenting the signatures of the offloadable methods and the necessary codes building a connection with the cloudlet. It requires adding the necessary code at the beginning of each offloadable method. The *ICEMobileDecisionMap* object contains the offloading decision of each offloadable method. It is obtained from the optimization result text file, kept into the mobile device memory, and in the form of a Java Hash Map object having <*key*, *value*> pairs.

IV. Experiments and Results

A. Hardware and Software Specifications of the Implementation Environment

The backend server is a computer with 4 cores of Intel i7 4th generation x64 microprocessor and a RAM with 8GB DDR3 capacity. Apache Tomcat provides the web server functionality by listening incoming requests. As the mobile client device, we used an LG G3 smartphone having Android Kitkat 4.4.2 OS, a Qualcomm Snapdragon 801 microprocessor with quad core processors hardware and a 3GB RAM. In order to create client/server communication, we included the Lipe-RMI for RMI-based offloading. In all of our three implementations, the mobile device and the server are connected to the same LAN. The bandwidth measurement tests reveal that LAN bandwidth is approximately 64% higher than the WAN bandwidth.

B. Scenarios with Mathematical Calculations

As the first demonstrative numerical example, in the client side, we implemented several matrix operations, including matrix creation with random values, addition, multiplication, division and inverse operations at matrices of different sizes. These mathematical operations use JScience mathematical library. In the server side, we developed backend server software in Java, which contains the same methods of the Android application with the same JScience library.

Fig. 2 depicts the call graph of these implementations. The first node initiates the application flow after getting an input from the user. The vertical flows are differentiated based on the matrix size. Among all the operations, matrix creation and matrix addition were found as the easiest operations to be completed by the device. On the other hand, there is a significant challenge when mobile devices perform multiplication, division and inverse operations.

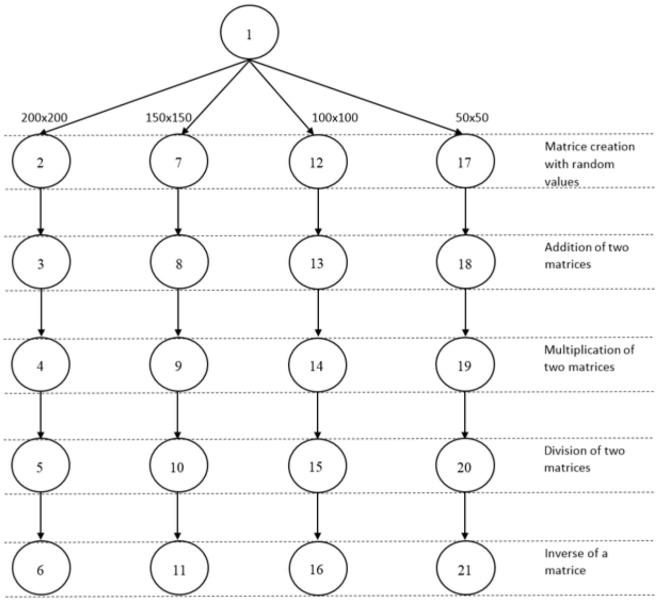


Figure 2. Call Graph of Matrices Calculations

TABLE I. MEASURED TIME AND ENERGY COSTS OF THE COMPARISON OF OBTAINED ENERGY EFFICIENCY

node id	T_n^l	T_n^r	$B_{m,n}$	E_n^l	$C_{m,n}$
1	-	-	-	-	-
2	50	52	695	35,8	720
3	4	1	2020	2,8	680
4	328	25	2100	114,6	700
5	72699	700	2515	44556	700
6	73206	614	1832	42350	800
7	35	21	520	20	700
8	4	10	1010	7,9	700
9	162	15	1210	58,1	700
10	30260	284	1400	19200	700
11	29539	270	1170	15950	700
12	15	12	320	5	700
13	1	2	585	3,2	700
14	80	6	450	6,9	700
15	8643	89	575	4600	780
16	8889	89	685	4700	700
17	2	2	242	5,4	700
18	1	2	124	0,6	760
19	14	2	107	29,8	700
20	1107	14	128	801	700
21	1076	9	97	450	700

For each scenario with different matrix size, we measured time and energy costs of each component of the call graph (Table 1). T_n^l represents the time that a node takes to execute the method locally, while T_n^r identifies the time that a node takes to execute the method remotely. $B_{m,n}$ describes the time that is required to transfer the necessary program state when m calls n. E_n^l shows the energy required to execute the method locally for each node n, $n \in N$. $C_{m,n}$ represents the energy that is required to transfer the necessary program state when m calls n. We generated two different scenarios. In the first one, all of the nodes are marked as offloadable except the root node; while in the second one several nodes are marked as non-offloadable.

Scenario 1: Unconstrained Offloading

For this case, we mark all the nodes as offloadable except the first one. If a node requires taking user input or accessing to a native device component, that node cannot be offloaded. For this scenario, the optimization solver resulted that it is better to offload 16 of 21 nodes to have maximum energy saving on mobile device. In that case, the nodes 3, 8, 13 and 18 will be offloaded to the cloudlet, together with their consecutive invocations. Since the objective is to maximize the energy saving in mobile device; even though the time performances of mobile device and cloudlet are equal to each other for any node, the optimization solver prefers offloading.

TABLE II. COMPARISON OF OBTAINED ENERGY EFFICIENCY

	Total Energy Cost (mJ)	**The Energy Gain (mJ)**	**Percentage of Gain**
Without Offloading	132.906	0	0%
Unconstrained Offloading	2.874	130.032	98%
Constrained Offloading	72.826	60.080	45%

The optimization function starts to offload with the lightweight nodes instead of the nodes having high energy cost while transferring. After transferring the node with lowest cost, the consecutive ones will not consume any energy, since they are already on the cloudlet, so they will be operated on the cloudlet. This example shows that the optimization function examines all of the nodes in high level, rather than considering it node by node. Since the set of mathematical operations are the same in each vertical flow with different size of matrices, the pattern is occurred in the same way. We can conclude that the position of the nodes and their invocations have significant effects on the offloading decision.

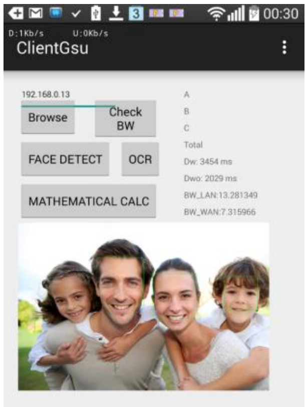
Scenario 2: Constrained Offloading

In order to discover the effect of node offloadability, we modified the first scenario by marking the nodes of 5, 10, 15 and 20 as not-offloadable in addition to the node 1. In this case, since the former methods of non-offloadable nodes are not resource-intensive, the optimization function decides offloading their consecutive nodes (6, 11, 16 and 21), which are relatively heavy tasks for the mobile device.

For these two scenarios, the total costs and obtained energy gains are summarized in Table 2. The total cost represents the sum of energy weights, when there is a mobile processing. The energy gain describes obtained energy saving via offloading. As a result, we observe that it is possible to achieve an energy saving up to 98% in *unconstrained offloading* and 45% in *constrained offloading* by integrating ICEMobile framework on the mobile device.

C. *Scenarios with Face Detection*

This is one of the most commonly applied scenarios for the mobile cloud computing, that identifies human faces in a given photo. Even though it seems as a quite simple image processing operation, it may become a highly computation-intensive operation proportional to the image resolution. As image processing library, we use the native Android FFTE face detection API. Our reason for choosing FFTE rather than OpenCV Android SDK is that the APIs of OpenCV do not detect faces of a static image. Instead, they make the face detection when there is an actual streaming on the camera [7]. Fig. 3 shows the screenshot of our developed Android application. The user selects a photo from the hard drive and then selects face detection function. The operation is performed on mobile device or on synchronized cloudlet. Then, the faces are identified with green rectangles based on their coordinate values. In the right side of the screen, the time cost is shown together with the detailed information about the call graph.



192.168.0.13

A
B
C
Total
Dw: 3454 ms
Dwo: 2029 ms
BW_LAN:13.281349
BW_WAN:7.315966

Figure 3. Screenshot of Face Detection Application

As the example, an image containing four human faces is chosen and it is resized to obtain multiple images of different size of pixels. The main reason of duplicating an image in different sizes is to eliminate other parameters, such as RGB values of the pixels, which could affect the test performance. Table 3 summarizes general properties of the images. In the table, the total number of pixels describes the multiplication of the width and height values.

The proposed offloading capability is integrated into the face detection application (Fig. 4). The figure represents the flow of on-device and cloudlet-based processing. The first and last nodes of two processing types are the same. However, in the second node of cloudlet-based processing (B^1), there is a conversion to raw data with Base64 encoding before transmitting the image data. Then in node C^1, the necessary initializations for socket, REST or RMI are completed. The node C^2 is the only node that is executed on the cloudlet and performs decoding and face detection operation. At the end of its execution, node C^2 sends obtained results back to the mobile device.

TABLE III. IMAGES WITH DIFFERENT DIMENSIONS FOR FACE DETECTION

	Width	**Height**	**Total # of Pixels**	**Size on Disk**
Image1	720	480	0.3 M	102 KB
Image2	1440	960	1.3 M	321 KB
Image3	2880	1920	5.5 M	980 KB
Image4	5760	3840	22.1 M	3410 MB

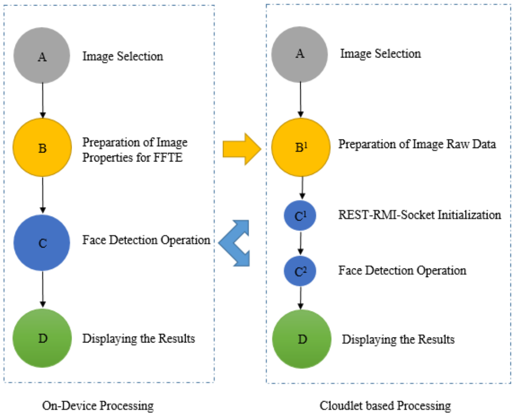


Figure 4. Call Graph Transformation of Face Detection

The tests of on-device processing reveal that the execution of native Android FFTE method takes more than 80% of total energy consumption. Since it is a native function, we are unable to partition this function to obtain a balanced distribution. As a result, we concluded that this use case is not ideal for optimization-based offloading. Fig. 5 shows that offloading will save energy for the images that are larger than 0.3 megapixels. We made use of this scenario to analyze different client/server communication techniques including Java sockets, RESTful Web Services and LipeRMI to explore the most efficient offloading model.

REST, socket and RMI-based communications are amongst the well-known offloading techniques. In order to compare the time and energy consumption of these communication types, we isolated the data transmission process of the use case, which starts by sending the data packet from client to server and finishes by receiving it back from server. (i.e., the edges $B^1 \rightarrow C^1$ and $C^2 \rightarrow D$ in Fig. 4).

We executed the operations for 10 times, and calculated the average of measured values. The energy consumption is measured in mW, and the time is measured in ms. As a result, as shown in Fig. 6 and Fig. 7, we observe that REST and socket-based offloading consume nearly the same amount of time and energy. Lipe-RMI is found more costly than REST and socket-based communications, besides its advantages of offloading.

ISBN: 978-1-61208-503-6

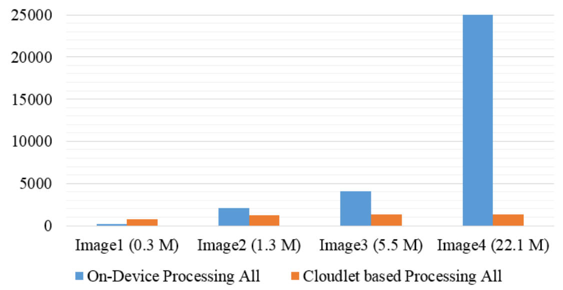


Figure 5. Comparison of Energy Consumption of Face Detection Operation

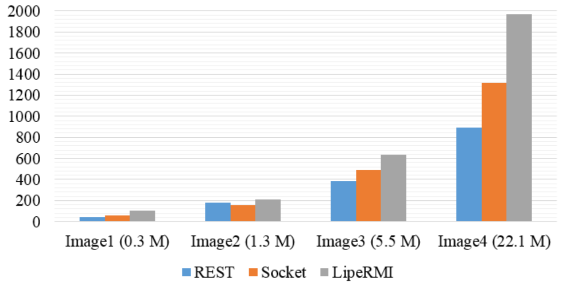


Figure 6. Comparison Based on Time Consumption

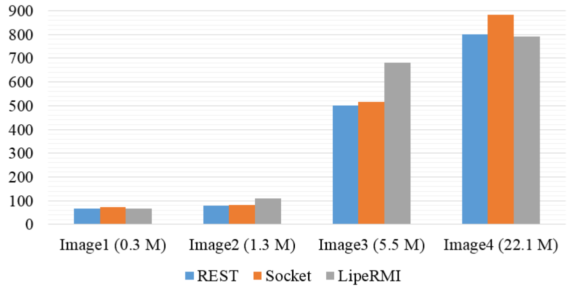


Figure 7. Comparison Based on Energy Consumption

D. Scenarios with OCR

As another use case, the ICEMobile framework is integrated into the Optical Character Recognition (OCR) application. The face detection and OCR are similar scenarios due to the fact that there is an image processing in each use case by using native functions. Hence, their call graph transformation is generated similarly (Fig. 4). The tests of on-device processing reveal that the execution of the *nativeGetUTF8Text* operation takes nearly 90% of total time and energy cost. It is much higher than the face detection operation, because there is not any painting operation on the image in OCR. Since Tesseract is not a Java-based library, we are unable to get into the structure of its API (*nativeGetUTF8Text*), and it becomes impossible to obtain a balanced distribution. We concluded that, the optimization model is not needed for this use case. Fig. 8 shows that offloading will save energy for images having more than 600 characters.

V. Conclusion

In this research, we first presented the challenges in mobile cloud computing and then focused on the usage of cloudlets as a solution for increasing energy efficiency of mobile devices. Cloudlets enable time and energy efficiency compared to distant clouds during the execution of computation-intensive tasks. In this paper, we implemented a lightweight RMI-based computation offloading in Java-based client and server. In order to examine the applicability of the proposed framework, we created three groups of synthetic test scenarios. Related call graphs are generated for each scenario. Detailed energy consumption analysis is done using a mobile application, PowerTutor. These values are utilized as the input of the optimization function. The results show that ICEMobile allows saving up to 98% of energy on mobile devices in specific cases, together with keeping the level of mobile user experience.

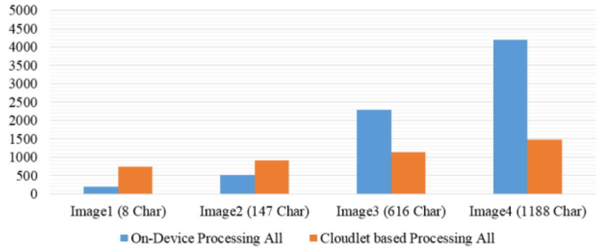


Figure 8. Comparison of on Energy Consumption of OCR Operation

Acknowledgments

This work is supported by Galatasaray University Research Fund, under the grant number 15.401.005.

References

[1] B. Zhou, A.V. Dastjerdi, R.N. Calheiros, S.N. Srirama and R Buyya, “A Context Sensitive Offloading Schme for Mobile Cloud Computing Service”, The Eighth International Conference on Cloud Computing (CLOUD), New York, USA, pp. 869-876, 2015, ISSN: 2159-6182.

[2] P. Mell and T. Grance, “The NIST definition of cloud computing”, US National Institute of Science and Technology, 2011, URL: http://dx.doi.org/10.6028/NIST.SP.800-145 (accessed on 21st December)

[3] M. Satyanarayanan, P. Bahl, R. Caceres and N. Davies, “The Case for VM-Based Cloudlets in Mobile Computing”, IEEE Pervasive Computing, vol.8(4):3, pp.14-23, Dec. 2009, doi: 10.1109/MPRV.2009.82.

[4] E. Cuervo, et al., “MAUI: Making Smartphones Last Longer with Code Offload”, The Eighth ACM MobiSys, pp.49-62, 2010, ISBN: 978-1-60558-985-5.

[5] B. Chun and P. Maniatis, “Augmented Smartphone Applications Through Clone Cloud Execution”, The Eighth Workshop on Hot Topics in Operating Systems (HotOS), pp.8-8, 2009. URL: https://www.usenix.org/legacy/event/hotos09/tech/full_papers/chun/chun.pdf (accessed on 15th November)

[6] R. Kemp, N. Palmer, T. Kielmann and H. Bal, “Cuckoo: a computation offloading framework for smartphones”, The Second International Conference on Mobile Computing, Applications, and Services, MobiCASE., pp.59-79, 2010, ISSN: 1867-8211, ISBN: 978-1-4673-7286-2.

[7] OpenCV4Android SDK, http://opencv.org/platforms/android.html (accessed on 27th December 2015).

Application Scenario of BIM-GIS Test-bed Implementation for Facility Management

Ji-Eun Kim Chang-Hee Hong
ICT Convergence and Integration Research Institute
Korea Institute of Civil engineering and Building Technology
Gyeonggi-Do, Korea
e-mail: jekim@kict.re.kr chhong@kict.re.kr

***Abstract*—According to people stay inside longer, an importance of Facility Management (FM) is getting higher. This is one of main factor relating a cost reduction. Building Information Modeling (BIM) contains object-based geometry & property data, and it is able to offer the personalized data with 3D viewing. This research relates BIM what is dealing with indoor data to Geographic Information System (GIS) what is dealing with outdoor data. Based on this, the research proposes an application scenario of BIM-GIS test-bed implementation for FM.**

Keywords-Building Information Modeling (BIM); Geographic Information System (GIS); Open platform; Test-bed; FM.

I. INTRODUCTION

Recently, the cost of maintenance after completion in a life cycle of building has been significant as to building owner and resident as well as the cost until completion. Even the well-constructed building, which is substantial and designed fashionably is important, to manage and operate building effectively after completion is one of the main factors relating to the long-term cost directly [1]. So, the various cases and studies about Facility Management (FM) system of existed buildings have been increasing.

The integration between Building Information Modeling (BIM) data including geometry/property information and Geometry Information System (GIS) including location information is appropriate to operate FM data based on city/building. It offers an object-based 3D visualization data and supports an easy operation management for sites, which includes several facilities on map-based system. BIM on GIS platform, which has been developed at Korea Institute of Civil Engineering and Building Technology (KICT), provides these services and it can handle the securement of data interoperability BIM and GIS, the visualization of 3D data, the light-weight algorithm for large scale data, and others [2][3].

This study builds the test-bed for substantiation of developed technology, and proposes the scenario for FM with BIM on GIS platform, as shown in Fig. 1. It aims four goals; BIM-GIS DB structure, BIM-GIS based 3D BIM modeling, Application scenario using BIM-GIS test-bed and verification & test-bed operation. These technologies are implemented on 'BIM on GIS platform', in Section 3.

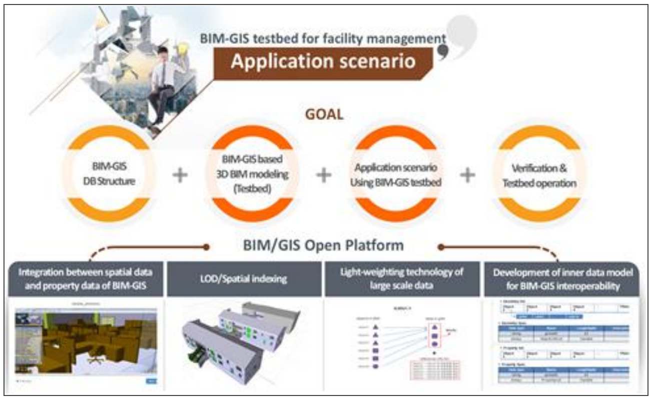

BIM-GIS testbed for facility management
Application scenario
GOAL
BIM-GIS DB Structure
+
BIM-GIS based 3D BIM modeling (Testbed)
+
Application scenario Using BIM-GIS testbed
+
Verification & Testbed operation
BIM/GIS Open Platform
Integration between spatial data and property data of BIM-GIS
LOD/Spatial indexing
Light-weighting technology of large scale data
Development of inner data model for BIM-GIS interoperability

Figure 1. Research overview

In Section 2, we analyzed a research trends: BIM/GIS integration and BIM-based FM in domestic/abroad. In Section 3, BIM on GIS platform was introduced, which has been developed at KICT for 5 years, and it is a foundation of this research. In Section 4, we constructed BIM/GIS test-bed, and it was processed as follow, 1) modeling of geometry and property data, 2) construction of BIM/GIS FM DB, and 3) shooting UAV and construction of true ortho-images. In Section 5, we designed of use-case scenario for facility management, firefighting and energy consumption. Finally Conclusion and Future work were proposed.

II. RESEARCH TRENDS

This study analyzed the research trends of BIM/GIS integration and BIM-based FM in domestic/abroad. Kang, T. W. et al [4] studied the software architecture for effective BIM/GIS based facility management data integration. For interoperability between two different data, it proposes BIM/GIS-based information for Extract, Transform, and Load architecture and tested it. Berlo, L. van et al [5] developed the CityGML GeoBIM Extension to get semantic IFC data into GIS context for integration of BIM and GIS. Niu, S. et al [6] proposed the solutions for data conversion of integration between BIM and GIS, and developed a BIM/GIS integrated web-based building energy data visualization system. Wetzel, E. M. et al [7] studied a BIM-based framework to support safe maintenance and repair practices for facility management. It also proposes the data processing and rule-based decision making with safety attribute identification and classification. Lee, K. S. [8] deducted BIM applicable elements according to related legal system, present technical level of BIM, and the requirement of FM for BIM utilization in the maintenance of urban metro facility.

Most of above researches approaches focus preponderantly the development of algorithm for enhancing interoperability BIM/GIS and the process or framework of BIM-based FM. According to increase of the importance for maintenance, there are various attempts to improve the problem about existing inefficient FM process. Thus, in this study, we have two goals, one is to construct the test-bed targeting real site by BIM modeling software (Revit Architecture) and verify it with BIM on GIS platform [2][3]. The next step is to extend availability of FM with scenarios.

III. INTRODUCTION OF BIM ON GIS PLATFORM

ICT Convergence and Integration Research Institute, KICT has been performing the study “Development of Open Platform for Interoperability between BIM and GIS” (2012.01~2016.12, total 5 years), which is one of main researches in KICT. This study develops BIM on GIS platform based on open source. Also, the element technology and information flow, which can apply indoor/outdoor spatial data effectively to the phase after construction are developed through 3D spatial data establishment for facility management and operation (Fig. 1, Fig. 2).

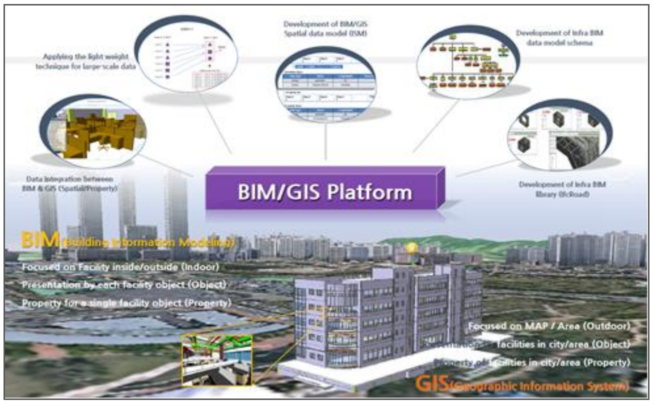

Applying the light weight technique for large-scale data
Development of BIM/GIS Spatial data model (SSM)
Development of Infra BIM data model schema
Data Integration between BIM & GIS (Spatial/Property)
BIM/GIS Platform
Development of Infra BIM library (IfcRoad)
BIM(Building Information Modeling)
Focused on Facility inside/outside (Indoor)
Presentation by each facility object (Object)
Property for a single facility object (Property)
Focused on MAP / Area (Outdoor)
facilities in city/area (Object)
Property of facilities in city/area (Property)
GIS(Geographic Information System)

Figure 2. Overview of BIM on GIS platform

In Korea, recently, several government agencies and institutions like Ministry of Land, Infrastructure and Transport, Seoul Metropolitan Government, Ministry of Public Safety and Security, Korea Land & Housing Corporation, and so on have made plans and tried to offer useful services integrating BIM for indoor spatial data and GIS for outdoor (city) data. As there are growing interests in the availability of BIM on GIS platform technology, and the use-case and possibility are required through this study.

IV. CONSTRUCTION OF BIM/GIS TEST-BED

For location of test-bed, we decided three places: main headquarter of KICT where is mainly composed of official buildings and facilities, and Fire Research Institute and Ricer Experiment Center where are composed of test laboratories & test buildings. Each place was planned for BIM/GIS modeling, working process of DB construction and development of operating technology.

First of all, 3D architectural modeling data was designed with data gathering and field survey based on existing 2D drawing plan, documents of facility history management. Also MEP and main research equipment were modeled with 3D BIM/GIS data. Then to visualize the effective 3D model, we shoot aerial images and built DSM data, and completed the test-bed modeling. The architecture of BIM/GIS test-bed was processed as follow, 1) modeling of geometry and property data, 2) construction of BIM/GIS FM DB, and 3) shooting UAV and construction of true ortho-images.

A. Modeling of BIM/GIS geometry/property data and FM-DB Construction

Beginning construction of satellite/aerial image, which was based on the platform, we worked the confirmation of site boundary/name, POI, standard classification system, basic property data, site survey, and actual images. Then based on these, we modeled BIM main data and building shape data with texturing according to Level of Detail (LOD). After that, main MEP and structure BIM modeling was worked, and all data was exchanged to Industry Foundation Classes (IFC), which BIM standard format for data verification. Finally through data converting, last data was loaded on BIM on GIS platform with inner format for interoperability.

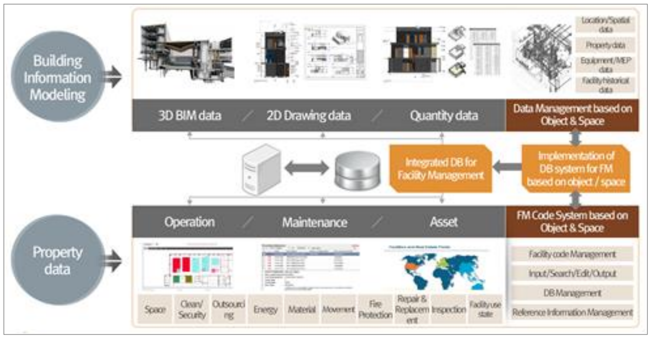


Figure 3. BIM/GIS Property data modeling process based on 3D architectural drawing

Fig. 3 shows the modeling process of BIM/GIS property data based on 3D architectural drawing. 3D BIM data was designed by 2D drawing and existed FM data. About the parts of non-updated like newly-built, extension, remodeling, we took photos with camera and drone. In the case of property data, we selected the main tasks among various FM works (space, clean and security, outsourcing, energy, material, movement, etc.), and connected data for operation, maintenance, asset with FM code system based on object and space. The DB structure was built with managing data (position data, spatial data, property data, equipment data, history data, etc.) by object and space, and saved at integrated DB for FM. Fig. 4 is an output of mapping images.

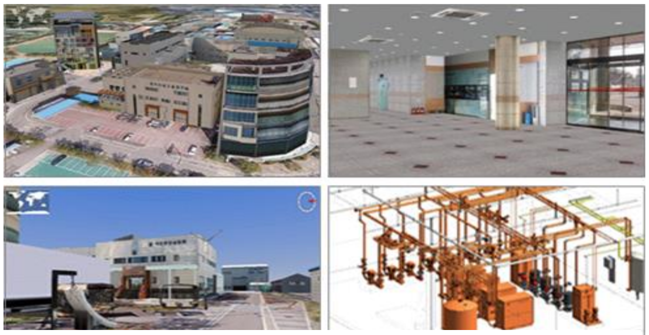


Figure 4. Output of mapping images to BIM/GIS modeling data

B. *Mapping UAV and True ortho-images*

The texturing of building shape like Google Earth, V-World makes BIM modeling image more realistic than before. To relate Image data by drone, shooting UAV and field survey to above BIM/GIS modeling data, we produced texture map with edited photography/distorted images. Finally, BIM/GIS modeling data and well-made image data were matched together.

V. Design of use-case scenario

Test-bed for BIM on GIS platform is able to manage by BIM object unit. This study reflected user requirements from KICT FM manager in priority to develop the system, which is adaptable in working-level. We discussed with FM team periodically about a current working process and designed the useful scenario based on this.

Data acquisition and deduction of requirements were much important to object-based FM system. We adopted many issues from analysis of other FM systems; therefore, designed the scenarios for long-term application. The scenarios would be proposed for three phases: FM, Firefighting, and Energy.

A. *Facility Management*

The scenario for facility management is as follows. To design it, we checked current KICT situation and FM process targeting KICT headquarter with FM manager. DB was constructed according to each work based on field survey, and FM data would be managed by space/floor/building unit (Fig. 5).

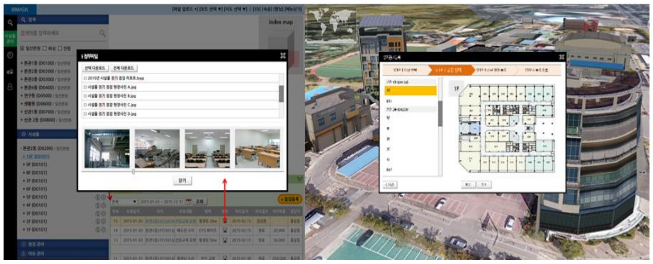


Figure 5. User Interface of BIM on GIS platform for FM

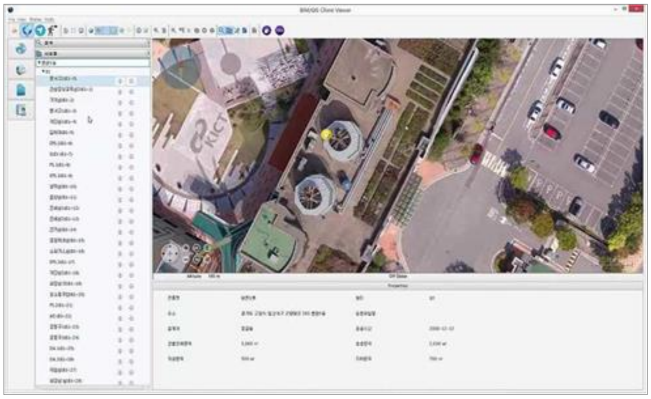


Figure 6. Searching facility lists by building unit

This can search and show data depending on user’s objective systematically by applying hierarchical order of space-floor-building-area (Fig. 6). And also based on existing KICT portal system, the scenario makes FM manager to Search/Read/Edit/Check with fundamental basic functions. The general users including FM manager can control a room schedule, a history management of joint equipment, site navigation, remodeling plan of institute, and so on because of object-oriented BIM modeling data. This FM process and FM system based on platform will be affiliated with KICT main system.

B. *Firefighting*

The scenario for facility firefighting can provide data of relevant building and site to fire department before they arrive at site, and it makes them to handle the place quickly with advance information. When a fire breaks out in the KICT headquarter, the alarm and warning sign operate, and firefighting system in BIM on GIS platform shows the spot (building) where the accident takes place automatically.

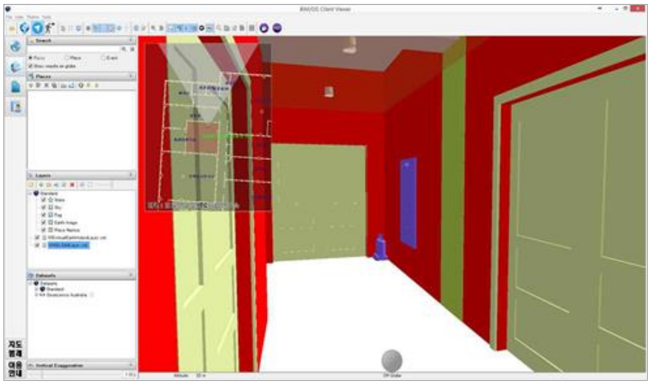


Figure 7. Visualization of firefighting objects

To understand clearly for firefighters, the platform turns out and shows from general architectural 3D model to structural 3D model, (Fig. 7). In the event of fire, firefighters generally should figure out the building structure with 2D drawings and analyze which objects are bearing structure for evacuation route and a rescue operation. These information are transmitted from BIM on GIS platform to firefighters as soon as case of fire.

This special model is composed of main structure objects from general 3D model with algorithm. As the purpose of data application, the structural model is able to visualize by objects and 2D/3D drawing of relating floors. Also this system analyzes and informs the path of emergency exit route from the spot to people. The simulation for fire drill usually can be worked.

C. Energy consumption

This scenario is for visualizing the energy consumption of each building in test-bed through sensors, which are situated at buildings before. When user converts a default mode into an energy consumption mode, basically the number of consumption is shown by sites with table or graph (Fig. 8). As selecting the site where the user wants to manage, the results are monitored in real time with space/floor/building/site for usage.

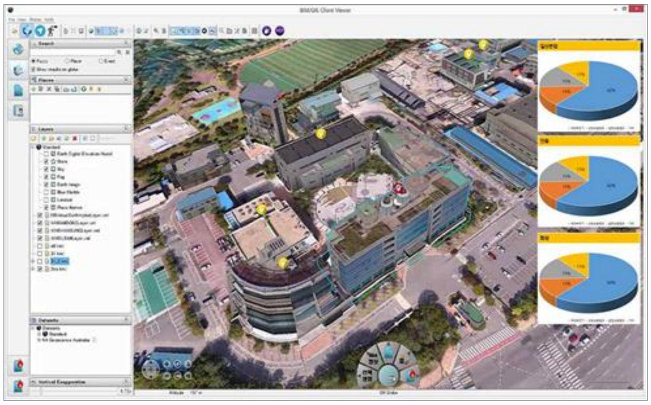


Figure 8. Searching for energy consumption of buildings

When a problem of sensor, energy manager can confirm the position of sensors with 3D model directly and take a measure soon. Also in case of unusual symptom for some building, this system can help the manager figuring out reasons with last statistics data (consumption number, records, etc.).

VI. Conclusion and Future Work

This study designed the test-bed for verification of BIM on GIS platform application and considered the use-case scenario for FM, firefighting, and energy consumption. In the future, as well as BIM on GIS platform, the needs of indoor spatial data are expected to rise integrating with VR/AR, smart city, etc. The most important thing is what users want to do. Considering the specific purposes of users as well as various fields requiring indoor-outdoor spatial data, the system has to apply and develop.

Acknowledgements

This research was supported by a grant from a Strategic Research Project (Development of BIM/GIS Interoperability Open-Platform 2016) funded by the Korea Institute of Civil engineering and Building Technology.

References

[1] Autodesk, “AS10660: How a Data Center Facility Owner Changed the Failing BIM Project into a Successful Project”, Technical report, http://au.autodesk.com/au-online/classes-on-demand/class-catalog/2015/revit-for-construction/as10660, 2015.

[2] Korea Institute of Civil engineering and Building Technology, “Development of Open Platform for Interoperability between BIM and GIS”, Research report, 2015.

[3] Korea Institute of Civil engineering and Building Technology, “Establishment of Test-bed and Pilot Model for Application Demonstration using BIM/GIS Platform”, Research report, 2015.

[4] T. W. Kang and C. H. Hong. “A study on software architecture for effective BIM/GIS-based facility management data integration”, Automation In Construction, vol.54, pp. 25-38, 2015.

[5] L. van Berlo and R. Berlo, “Integration of BIM and GIS: The development of the CityGML GeoBIM extension”, Advances in 3D Geo-Information Sciences, pp. 211-225, 2011.

[6] S. Niu, W. Pan, and Y. Zhao, “A BIM/GIS Integrated Web-based Visualization System for Low Energy Building Design”, Procedia Engineering, vol.121, pp. 2184-2194, 2015.

[7] E. M. Wetzel and W. Y. Thabet, “The use of a BIM-based framework to support safe facility management processes”, Automation In Construction, vol.60, pp. 12-24, 2015.

[8] K. S. Lee, “(A)study on the application of BIM elements in the procurement phase for BIM utilization in the maintenance of urban metro facility”, Master thesis, Hanyang University, Korea, 2013.

Smart Data Pricing Model for Intelligent Transportation Systems

S. Emre Alptekin

Galatasaray University
Department of Industrial Engineering
Istanbul, Turkey
email: ealptekin@gsu.edu.tr

***Abstract*- Internet of Things is a novel paradigm that foresees Internet-connected devices generating constantly new data using sensors/actuators. The gathered data from various sources facilitates new ways of integration and operations that are essential for developing systems, such as intelligent transportation management. Intelligently managing an infrastructure like traffic systems is expected to contribute to overall safety, economical development and environmental sustainability. However, its success depends on users' willingness to share with and use data provided by the platform. Therefore, there should be mechanisms to be put in place, which will motivate latent customers/contributors and furthermore manage efficiently the flow of data on possibly stringent network conditions. Smart data pricing, a concept that aims to give users the right economic incentives and manage network congestion in high demand periods, is providing an effective solution for this problem. In this paper, models based on game theory is used to deal with data pricing. The applied model takes into account the level of service quality and the sensitivity of the customers on price levels and quality. The applicability of the proposed methodology is demonstrated via a case study.**

***Keywords*- Internet of Things; dynamic pricing; game theory; mobile cloud computing.**

I. Introduction

The Internet of Things (IoT), a revolutionizing approach foreseeing "smart, connected" products is promising its early adaptors new competitive opportunities and is seen as a disruptive technology [1]. There are several prominent organizations, such as Google, General Electric, Amazon, Samsung, etc. coming with their own view of the concept. It is basically a new model that has its roots based on ever advancing wireless communications along with the artificial intelligence framework that is expected to enhance the experience of the users. From the end users' perspective, the whole experience of IoT should contribute especially in areas of assisted living, e-health, enhanced learning and from the business users' perspective in fields, such as automation, industrial manufacturing, logistics, business/process management, intelligent transportation of people and goods [2].

As it is with every newly emerging technology, the IoT vision requires that organizations should develop beyond traditional mobile computing scenarios and propose products that should connect everyday existing objects and embed somehow intelligence into their offerings [3]. As proposed by [3], IoT demands: (1) a shared understanding of the situation of its users and their appliances, (2) software architectures and pervasive communication networks to process and convey the contextual information to where it is relevant, and (3) the analytics tools in the IoT that aim for autonomous and smart behavior. If the organizations are able to deliver in all these aspects the desired smart connectivity and context-aware computation should be the outcome.

Intelligent transportation systems enriched with IoT as suggested by Ibanez et al. [4] aim to achieve goals, such as safety and personal security, access and mobility, environmental sustainability, and economical development through minimizing CO2 emissions, improving traffic efficiency, and road safety, as well as reducing vehicle wear, transportation times and fuel consumption. However, developing such a framework necessitates integration of information and communication technologies that are usually treated as independent silos of automation. Prospects of possible integration anticipates large amount of data to be collected, processed and fed back on real-time if possible to the users' of the system. The main challenge for the adaptation of intelligent transportation systems is in the implementation of adequate and necessary technologies and infrastructures in vehicles, roads, streets and avenues [4].

However, new business opportunities created through processed information and delivered as a service to customers, may establish new revenue streams for service providers [5]. Effectively managing information and keeping quality of service levels under control in case of constrained network conditions necessitates new approaches, such as smart data pricing. Smart data pricing, a mechanism aiming to understand users' behaviors and adapting to different network traffic conditions is believed to be a solution for creating economic models for computing optimized prices [6]. Accordingly, service providers will have to develop economic models for price competition that should adapt to customers' expectations and network conditions.

In this work, an economic model for price competition among service provider in transportation networks is proposed. The model aims to analyze consumers' behaviors to changing prices and quality levels and tries to optimize service providers' revenues. The proposed framework is based on mathematical models of game theory.

The case study used to demonstrate the effectiveness of proposed methodology defines different scenarios. The aim is to examine the effect of different behaviors on the pricing and depict actions that should maximize revenue of the service providers.

The remaining part of the paper is organized as follows: in Section 2 related literature is given. Section 3 briefly describes the methodologies that constitute the proposed framework. The steps and details of the implementation into the intelligent transportation management problem is given in Section 4. Finally, Section 5 concludes the study.

II. Literature review

Internet of Things related literature covers different aspects of the topic, ranging from enabling technologies to protocols and possible application scenarios. Similarly, intelligent transportation systems related problems and propositions are very popular among research community. Some of the recent work that constituted the base of this study is presented in this section.

In their work, Ibáñez et al. [4] presented emerging technologies, such as connected vehicles, wireless technologies, etc. that will complement intelligent transportation systems. They showed using examples how cloud computing complements the development of transportation systems. They also discussed how IoT will contribute to seamless integration of different systems with the intention of more sustainable transportation solutions and improved road safety.

Niyato et al. [7] introduced an overview of IoT, its architecture, benefits and business models and proposed smart data pricing for IoT systems and services. They suggested a pricing scheme for IoT service providers taking into account sensing data buying and service subscription with bundling. They found out that in case of a coalition, multiple service providers could achieve a higher profit level.

Hoang and Niyato [5] developed an economic model for competitive pricing problem among information service providers in an Internet-of-Vehicle environment. They proposed a competitive repetitive game model to obtain prices for providers through Nash equilibrium solution. Using simulation results, they assessed the efficiency of their solution.

Sen et al. [6] proposed smart data pricing mechanisms to avoid network congestion by creating incentives to modify user behavior or shift demand to less congested times or to supplementary networks. They discussed two different scenarios: time-dependent pricing and traffic offloading and foreseen smart data pricing applied to machine-to-machine communication and IoT setting.

III. The Methodology

Smart data pricing concept describes pricing options applied by service providers to replace traditional flat-rate model. Typical models make use of mechanisms, such as, usage-based pricing / metering / throttling / capping, time / location / congestion-dependent pricing, app based pricing / sponsored access, Paris metro pricing, quota-aware content distribution, reverse billing or sponsored content [6]. Dynamic pricing approach as part of smart data pricing enables real-time pricing changes and ability to respond to network congestion and fluctuations in quality of experience of the users' of the system.

However, setting prices without considering the reactions of competition possibly underoptimizes the market share and utilities of service providers. However, answering questions like: "How can we decide what action to choose in a competitive environment?" and "What are other companies doing?" requires study of market conditions and behaviors of actors in the market [8].

Game theory defined as the formal study of conflict and cooperation provides a language to formulate, structure, analyze and understand strategic scenarios [9]. Game theory framework consists of theoretical methods of microeconomic origin and are used in many other areas of the economy and in a range of other social and behavioral sciences [10].

The basic requirements for establishing a game theoretical model necessitates definition of players, their preferences, their information, strategic actions available to them, and how they influence the outcome. At this point whether or not the players have the inclination or possibility of cooperation should also be defined.

There are several assumptions made at this stage and one of the most common one is that players are considered as rational. A rational player is defined as the one who always chooses an action that gives the result that is most preferred considering the expected reactions of its opponents.

The approach applied in this paper assumes non-cooperative games with rational actors. In game theory, typically solution approaches are based on Nash equilibrium concept, which is used to analyze the outcome of the strategic interaction of several decision makers. The Nash equilibrium tries to predict what will happen if several persons or institutions are making decisions at the same time, and if the result depends on the decisions of others. After having chosen strategies, no player should benefit by reconsidering his strategy while the other players keep all their strategies unchanged. If this is the case, the current set of strategic choices and corresponding utilities represent Nash equilibrium.

IV. Data Pricing Framework

A. *Proposed Model*

The game theoretical framework used in this paper is based on researches of Işıklar Alptekin and Bener [11] [12] and Demirci and Alptekin [13], who applied the same framework to revenue management in e-commerce. In their work Işıklar Alptekin and Bener [11] [12] considered short term sub-lease of unutilized spectrum bands to different service providers using a non-cooperative game theoretical model. As outcome of the game, they calculated the optimum prices of the offered frequency bands subject to QoS constraints. They concluded that the demand models must be chosen with great care, since the choice of its parameters has profound implications for the market equilibrium. Based on their research, the pricing problem for intelligent transportation system is formed as follows:

Players: data based service provider in intelligent transportation network

Actions and strategies: The choice of the price offering based on quality of experience levels

The main assumption of the model is service providers are competing with each other non-cooperatively and independently. The possible actions are defined as: the price of the service provided along with its quality level. The decision of the service providers and also the consumers are affected by the action of other service providers. The aim for the providers is typically profit maximization.

As mentioned in the previous section, game theoretical models are in search of a focal point, from which no player would deviate, i.e., a Nash equilibrium.

The pricing strategy set consists of a set of N service providers, SP_i, designated by $i = \{1,2, ..., N\}$. Each company has to define two sets of parameters: $(p,q) \in \mathcal{R}_+^{2N}$. $\boldsymbol{p} = \{\boldsymbol{p_{1k}}, \boldsymbol{p_2}, \dots, \boldsymbol{p_{Nk}}\}$ is the price vector and p_{ik} is the price that SP_i charges for each service provided to kth customer. The prices may be based on cloud resources used or value-added data services provided. $\boldsymbol{q} = \{\boldsymbol{q_{1k}}, \boldsymbol{q_{2k}}, \dots, \boldsymbol{q_{Nk}}\}$, is the experienced quality level of the services, where q_{ik} measures the quality offered by SP_i to kth customer.

The demand for each service provider is represented with $D_i(p,q)$: $\mathcal{R}_+^{2N} \to \mathcal{R}_+$. The model assumes that the demand of SP_i depends not only on its own parameters p_i and q_i, but also on the prices and quality level offered by its competitors. The utility function is defined as $U_{ik}(p,q)$: $\mathcal{R}_+^{2N} \to \mathcal{R}_+$. The strategy space of $S_{ik} \in \mathcal{R}^2$is defined as the subset of : [11]

$$S_{ik} = \{(p_{ik}, q_{ik}): 0 \le p_{ik}^{min} \le p_{ik} \le p_{ik}^{max} ; 0 \le q_{ik}^{min} \le q_{ik} \le q_{ik}^{max}\} \quad (1)$$

As suggested by [11] beyond some maximum price, demand will be zero whatever the prices and QoS levels of competitors are. Accordingly, the service provider has to define an upper bound on price. The lower bound is set so as to keep the net profit of the *SP* positive.

In this model, we assume that the average demand is linear in prices and thus given as a linear demand function in the following form [11]:

$$D_{ik}(p,q) = a_{ik} - b_{ik}.p_{ik} + \textstyle\sum_{j\in I, j\neq i} c_{ijkl}.p_{jk} + \beta_{ik}.q_{ik} - \textstyle\sum_{j\in I, j\neq i} \gamma_{ijkl}.q_{jk} \ge 0 \quad (2)$$

with a_{ik} defined as the base demand of kth customer from ith service provider and $b_{ik}, c_{ijkl}, \beta_{ik}, \gamma_{ijkl}$ are positive constants representing the extent to which customers are affected by changes in the price and quality. c_{ijkl} is the measure that shows how the lth customer is influenced by the price of SP_i to the kth costumer when lth customer is served by SP_k. The constants b and c should satisfy the following condition:

$$b_{ik} > \textstyle\sum_{j\neq i} c_{ijkl}, i, j \in I \text{ and } k, l \in I \quad (3)$$

The condition requires that the influence of a service providers' own price is larger on its own demand than the prices of its competitors. This is the typical scenario under the assumptions of loyalty or the imperfect knowledge of competitors' prices.

The demand function defined in the model assumes that the customers are aware of the service quality they are receiving and therefore are sensitive to quality changes. The parameters reflecting the sensibility to experienced quality levels are defined with parameters q_i and q_j, respectively. An objective calculation of the quality parameters should include service related performance metrics, such as bandwidth, response times, and resources dedicated to user, etc. In this paper, an experienced service level will be used for demonstration purposes.

Having defined the quality related parameters, the revenue of a service provider is calculated by multiplying its price with its demand:

$$U_i(p,q) = p_i.D_i(p,q) \quad (4)$$

When the demand function is replaced with the equation 2:

$$U_i\ (p,q) = p_i\ (a_{ik} - b_{ik}.p_{ik} + \textstyle\sum_{j\in I, j\neq i} c_{ijkl}.p_{jk} + \beta_{ik}.q_{ik} - \textstyle\sum_{j\in I, j\neq i} \gamma_{ijkl}.q_{jk} \quad (5)$$

At this stage, the existence and uniqueness of the equilibrium among service providers has to be proven.

As defined by [11], a single-parameter Nash equilibrium in *p* at *q* is the vector *p** that solves for all *i*:

$$U_i(p^*, q) = \max_{p_{ik}, q \in \mathcal{R}_i} U_i\left(p_{1k}^*, \cdots, p_{(i-1)k}^*, p_{ik}^*, p_{(i+1)k}^*, p_{Nk}^*, q\right) \quad (6)$$

In order to prove the Nash equilibrium the supermodularity of the game has be to shown. Supermodular games require that when a player takes additional actions, others want to do the same. The game *G* is defined to be supermodular if the following conditions are met [11]:

S_n is an interval of $\mathcal{R}^N$, where

$$S_n = [\underline{y_n}, \overline{y_n}] = \{x | \underline{y_n} \le x \le \overline{y_n}\} \quad (7)$$

f_n is twice continuously differentiable on S_n ;

$\frac{\partial^2 f_n}{\partial x_{ni} \partial x_{mj}} \ge 0$ for all n and all $1 \le i < j \le N$;

$\frac{\partial^2 f_n}{\partial x_{ni} \partial x_{mj}} \ge 0$ for all $n \neq m$, $1 \le i \le N$ and $1 \le j \le M$.

A pure Nash equilibrium is a strategy tuple $x = (x_n; n \in N)$, such that each x_n maximise $f(\hat{x}_n, x_{-n})$ over S_n. The strategic feasible set of the game is defined using the following formulation [11]:

$$S_i = \{p_i: 0 \leq p^{min} \leq p_i \leq p^{max}; i = 1,2, \dots, N\} \quad (8)$$

The partial derivatives of the utility function for prices and quality levels are calculated and given as:

$$\frac{\partial U_i(p,q)}{\partial p_i} = D_i(p,q) - b_i.p_i \quad (9)$$

$$\frac{\partial^2 U_i(p,q)}{\partial p_i^2} = -2b_i \leq 0 \quad (10)$$

$$\frac{\partial U_i(p,q)}{\partial q_i} = \beta_i.p_i \quad (11)$$

$$\frac{\partial^2 U_i(p,q)}{\partial q_i^2} = 0 \leq 0 \quad (12)$$

$$\frac{\partial^2 U_i(p,q)}{\partial p_i \partial p_j} = \sum_{i \neq j} c_{ij} \geq 0 \quad (13)$$

In order to find the prices that maximizes revenue, the derivative of the utility function is taken and set equal to zero:

$$\frac{\partial U_i\,(p,q)}{\partial p_i} = D_i(p,q) + p_i(-b_i) = 0 \quad (14)$$

$$\frac{\partial U_i\,(p,q)}{\partial p_i} = a_i - b_i.p_i + \sum_{j \in I, j \neq i} c_{ij}.p_j + \beta_i.q_i - \sum_{j \in I, j \neq i} \gamma_{ij}.q_j - b_i.p_i = 0 \quad (15)$$

$$\frac{\partial U_i\,(p,q)}{\partial p_i} = a_i - 2.b_i.p_i + \sum_{j \in I, j \neq i} c_{ij}.p_j + \beta_i.q_i - \sum_{j \in I, j \neq i} \gamma_{ij}.q_j = 0 \quad (16)$$

$$2.b_i.p_i - \sum_{j \in I, j \neq i} c_{ij}.p_j = a_i + \beta_i.q_i - \sum_{j \in I, j \neq i} \gamma_{ij}.q_j \quad (17)$$

As a linear system of equation in *p*, the equations can be represented in a matrix form.

$$Ap = \left[a_i + \beta_i.q_i - \sum_{j \in I, j \neq i} \gamma_{ij}.q_j\right] \quad (18)$$

$$A = \begin{pmatrix} 2b_1 & -c_{12} \cdots & -c_{1N} \\ -c_{(N-1)1} \vdots & \ddots & -c_{(N-1)N} \vdots \\ -c_{N1} & -c_{N2} \cdots & 2b_N \end{pmatrix} = \\ = \Phi(1 - T) \quad (19)$$

$$\Phi = diag(2b_1, 2b_2, \dots, 2b_N) \quad (20)$$

$$T = \begin{pmatrix} 0 & \cdots & \frac{c_{1N}}{2b_1} \\ \vdots & \ddots & \vdots \\ \frac{c_{N1}}{2b_N} & \cdots & 0 \end{pmatrix} \quad (21)$$

Hence, $A^{-1} = (I - T)^{-1}.\Phi^{-1}$ and optimum price at the equilibrium is defined as:

$$\text{p*}{=}A^{-1}.X = (I - T)^{-1}.\Phi^{-1}.X \quad (22)$$

with

$$X = a_i + \beta_i.q_i - \sum_{j \in I, j \neq i} \gamma_{ij}.q_j \quad (23)$$

$$p_i^* = \sum_{j=1}^{N} A_{ij}^{-1}.a_i + (A_{ii}^{-1}.\beta_i - \sum_{i \neq j} A_{ij}^{-1}.\gamma_{ji}).q_i + \sum_{j \neq i}(A_{ij}^{-1}.\beta_j - \sum_{l \neq j} A_{il}^{-1}.\gamma_{li}).q_j \quad (24)$$

The contraction approach that proves the uniqueness of the equilibrium defines the sufficient condition as below [11]:

$$\frac{\partial^2 U_i(p,q)}{\partial p_i^2} + \sum_{i \neq j} \left|\frac{\partial^2 U_i(p,q)}{\partial p_i \partial p_j}\right| < 0 \quad (25)$$

$$-2b_i + \sum_{i \neq j} c_{ij} < 0 \quad (26)$$

Therefore, if the conditions are met, the equation 24 will result in the optimum prices for *SP_i*.

B. Numerical Application

The applicability of the proposed model is demonstrated through a demonstrative example where two intelligent transportation system service providers with different experienced quality levels are competing in the same market.

The perceived quality levels along with the parameters used in the calculations are given in Table 1. *NP* denotes the service providers, *C* denotes the customers.

The parameters defined in Table 1 try to model a typical customer's sensitivity to the quality and prices of the services offered by the service providers given the quality and price of the competitors. Solving the formula given in 24, the Nash equilibrium price is p^* obtained.

TABLE I. THE VALUES OF THE PARAMETERS OF THE DEMAND FUNCTION

	NP_1		NP_2	
	C_1	C_2	C_1	C_2
β	4.5	4.5	3	3
$\gamma_{NP_1 \to C_1}$	0	1.5	0.8	0.5
$\gamma_{NP_2 \to C_1}$	1.5	0	0.5	0.8
$\gamma_{NP_1 \to C_2}$	1.3	1.4	0	1.1
$\gamma_{NP_2 \to C_2}$	1.4	1.3	1.1	0
b	4.5	4.5	7	7
$c_{NP_1 \to C_1}$	0	1.5	2.2	1.9
$c_{NP_2 \to C_1}$	1.5	0	1.9	2.2
$c_{NP_1 \to C_2}$	1.1	1.6	0	1.5
$c_{NP_2 \to C_2}$	1.6	1.1	1.5	0
q	0.75	0.75	0.85	0.85

For demonstrative purposes, the parameters used in the case study assume two customer profiles: a high profile customer (C_1) and a low profile customer (C_2). The base demand (a) is assumed to be the same for both customer profiles and is set at 20 for each. The base demand represents average demand of different customer profiles.

The following matrix is used to calculate the values of demand (D), the price (p^*), and the utility (U^*).

$$\boldsymbol{A} = \begin{pmatrix} 9 & -1.5 & -1.1 & -1.6 \\ -1.5 & 9 & -1.6 & -1.1 \\ -2.2 & -1.9 & 14 & -1.5 \\ -1.9 & -2.2 & -1.5 & 14 \end{pmatrix}$$

The formula given in 24 is used to obtain the results presented in Table 2.

TABLE II. OPTIMUM RESULTS FOR PRICE, DEMAND AND UTILITY

	$\boldsymbol{NP_1 \rightarrow C_1}$	$\boldsymbol{NP_2 \rightarrow C_1}$	$\boldsymbol{NP_1 \rightarrow C_2}$	$\boldsymbol{NP_2 \rightarrow C_2}$
$\boldsymbol{D}$	16.65	16.90	19.94	20.12
$\boldsymbol{p^*}$	3.70	3.76	2.85	2.87
$\boldsymbol{U^*}$	61.62	63.53	56.80	57.83

The effect of the changes in experienced quality level is shown in Table 3, where the quality level of the first service provider is increased to %100 and the quality level of the second service provider is decreased to 1%.

TABLE III. OPTIMUM RESULTS WITH THE CHANGE OF QUALITY LEVEL OF THE FIRST SERVICE PROVIDER

	$\boldsymbol{NP_1 \rightarrow C_1}$	$\boldsymbol{NP_2 \rightarrow C_1}$	$\boldsymbol{NP_1 \rightarrow C_2}$	$\boldsymbol{NP_2 \rightarrow C_2}$
$\boldsymbol{D}$	17.96	15.43	20.77	18.99
$\boldsymbol{p^*}$	3.99	3.43	2.97	2.71
$\boldsymbol{U^*}$	71.68	52.88	61.65	51.57

When the sensitivity for quality of the low profile customer is set as high profile customer, the following optimum results are obtained (Table 4).

TABLE IV. OPTIMUM RESULTS AFTER VARIATION OF THE SENSITIVITY FOR QUALITY OF THE LOW PROFILE CUSTOMER

	$\boldsymbol{NP_1 \rightarrow C_1}$	$\boldsymbol{NP_2 \rightarrow C_1}$	$\boldsymbol{NP_1 \rightarrow C_2}$	$\boldsymbol{NP_2 \rightarrow C_2}$
$\boldsymbol{D}$	16.83	17.08	20.67	20.92
$\boldsymbol{p^*}$	3.74	3.80	2.95	2.99
$\boldsymbol{U^*}$	62.94	64.85	61.03	62.49

In the opposite case where high profile customer is no longer sensitive to the quality, the following optimum results are obtained (Table 5).

The results of demonstrative examples show that demand and accordingly prices are changing when different sensibility values for quality are used. However, in real life scenarios setting the correct values for quality and price sensibility to different customers requires that their profile should be extracted from the relationship between customer and service providers using techniques, such as customer relationship management, big data analysis, etc. If correct profiles could be identified, the resulting pricing mechanism and hence the prices will be realistic.

TABLE V. OPTIMUM RESULTS AFTER VARIATION OF THE SENSITIVITY FOR QUALITY OF THE HIGH PROFILE CUSTOMER

	$F_1 \rightarrow A_1$	$F_2 \rightarrow A_1$	$F_1 \rightarrow A_2$	$F_2 \rightarrow A_2$
D	14.30	14.36	18.69	18.87
p^*	3.18	3.19	2.67	2.69
U^*	45.43	45.84	49.92	50.85

When the results presented in tables are analyzed, several conclusion could be drawn. For example, Table 3 reveals that demand of high profile customers to the first service provider has increased and the demand of the same customer to the second service provider has decreased, when the quality level of the first provider is increased and the second provider is decreased. Moreover, the price of the first service provider is increased for all customer profiles. Hence, the first service provider with its increased experienced quality level is able to increase its total utility, whereas the second service provider with its decreased utility potentially also lost revenue.

The effect of sensitivity levels of customer profiles is explored in Table 4 and Table 5. Here, the most striking finding is when a customer sacrifices his/her desire for quality, prices are falling. On the other hand, if all customers are becoming more sensitive to the quality, prices are increasing. Final finding is that the revenues of the service providers are increasing when all customers demand for a higher experienced level of quality and also accept paying more money.

V. CONCLUSION

Intelligent transportation systems with their expected benefits will shape the future traffic flow and contribute to sustainability of the communities and will be a potential life saver in cases of accident prevention. The proposed methodology in this paper aims to approach the intelligent transportation system from the service providers' perspective. As the system requires high amount of investment, pricing mechanisms that will contribute to the utilities of service providers and also manage the quality levels experienced by the system's customers are of great importance. Simple usage-based pricing mechanisms will be potentially infective under these circumstances. Pricing models related to time, related to demand or related to sensitivity/loyalty have the ability to respond to ever increasing awareness of customers of prices and quality levels in the marketplace.

However, setting the right price for different consumer profiles requires that the market properties are well captured. Especially, in order to know the customers, all necessary data about their buying habits, their sensitivity on certain factors and what they seek in the market should be explored meticulously. This process requires extensive data mining, which should produce the data needed to create efficient algorithms for pricing and setting the correct levels of quality.

Future work could explore more realistic scenarios where prices of services are accepted with different possibility levels by different customer profiles, which should reveal the dynamic structure of pricing mechanism better.

ACKNOWLEDGMENT

This research has been financially supported by Galatasaray University Research Fund, with the project number 15.402.005.

REFERENCES

[1] M.E. Porter, and J. E. Heppelmann, "How Smart, Connected Products Are Transforming Competition", Harvard Business Review, November Issue, pp. 1-23, 2014.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey", Computer Networks, Vol. 54, pp. 2787-2805, 2010.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, future directions", Future Generation Computer Systems, Vol. 29, pp. 1645-1660, 2013.

[4] J. A. G. Ibáñez, S. Zeadally, and J. C. Castillo, "Integration Challenges of Intelligent Transportation Systems with Connected Vehicle, Cloud Computing, and Internet of Things Technologies", IEEE Wireless Communications, December, pp. 122-128, 2015.

[5] D. T. Hoang, and D. Niyato, "Information Service Pricing Competition in Internet-of-Vehicle (IoV)", International Conference on Computing, Networking and Communications (ICNC), pp. 1-5, 2016.

[6] S. Sen, C. J. Wong, S. Ha, and M. Chiang, "Smart Data Pricing: Using Economics to Manage Network Congestion", Communications of the ACM, December, Vol. 58(12), pp. 86-93, 2015.

[7] D. Niyato et al., "Smart Data Pricing Models for the Internet of Things: A Bundling Strategy Approach", IEEE Network, March/April, pp. 18-25, 2016.

[8] K. S. Moorthy, "Using Game Theory to Model Competition", Journal of Marketing Research, 22(3), pp. 262-282, 1985.

[9] L. Theodore, and B. V. Turocy, "Game Theory", CDAM Research Report LSE-CDAM, London: London School of Economics, 2001.

[10] M. J. Osborne, "An Introduction to Game Theory", Oxford University Press, 2002.

[11] G. Işıklar Alptekin, and A. Bener, "An efficient spectrum management mechanism for cognitive radio networks", IFIP/IEEE International Symposium on Integrated Network Management, pp. 653-660, 2009.

[12] G. Işıklar Alptekin, and A. Bener, "Spectrum Trading in Cognitive Radio Networks with Strict Transmission Power Control", European Transactions on Telecommunications, pp. 282-295, 2011.

[13] B. Demirci, and S. E. Alptekin, "Revenue Management in E-Commerce: A Case Study", International MultiConference of Engineers and Computer Scientists, Vol II., pp 1-6, 2013.