A Novel Abnormal Behavior Detection Framework to Maximize the Availability in Smart Grid

Incheol Shin*

Abstract

A large volume of research has been devoted to the development of security tools for protecting the Smart Grid systems, however the most of them have not taken the Availability, Integrity, Confidentiality (AIC) security triad model, not like CIA triad model in traditional Information Technology (IT) systems, into account the security measures for the electricity control systems. Thus, this study would propose a novel security framework, an abnormal behavior detection system, to maximize the availability of the control systems by considering a unique set of characteristics of the systems.

Keywords : Smart Grid|Security|Abnormal Behavior Detection|Cyber-Physical Attacks

I. INTRODUCTION

The Smart Grid initiative aims to propel utilities and their electricity delivery systems into the 21st century with the aid of various information and communication technologies. A wide range of different control devices/systems will be interconnected through the internet and peer-to-peer connections as well as the closed networks like those used in the Smart Grid infrastructures. That is, not only the internet can be attacked, but the devices and networks at the Smart Grid systems that controls the electrical power grids can also serve as an attack vector, eventually. One of the most noticeable and important key difference between the Smart Grid systems and ICT (Information Communications Technology) in terms of security dimension is the priority on the availability in the security triad, CIA in the Internet and AIC in the control systems. However, most of the current researches on developing security countermeasures against cyber threats to Smart Grid systems have employed the best practices associated with CIA triad security model, in order of importance from ICT based security system designs, without consideration of the Smart Grid security requirements. In accordance with Isaac Ghansah in [1] and the guidelines for the Smart Grid security from [6] and [7], the security systems for the Smart Grid systems, advanced electrical power grid systems or control systems in one of the critical infrastructures, should be able to guarantee the availability of the system operation with priority than the other two factors. The availability of the control systems is defined in identifying and assuring data and critical services that require to be usable or ready for certain purposes at a very specific time restrictions. Securing the Smart Grid systems should be based on the three fundamental dimensions of AIC in order since the control networks in the critical infrastructure like the Smart Grid networks carry not only information but also control messages to support the grid automation, while the ICT networks, like the Internet, deliver the information only. That is, security frameworks for the electrical control systems against various cyber-physical attacks should embed these natures based on the AIC security triad. In other words, security systems for the Smart Grid should not merely isolate adversarial or suspicious network traffic like the way that the systems for the ICT networks simply do, but estimation of the impacts from the control network breaches should be preceded for the further security actions to maintain

* This Research was supported(in part) by Research Funds of Mokpo National University in 2015
*Member, Mokpo National University

Manuscript : 2017. 08. 08
Revised : 2017. 09. 04, 2017. 09. 25
Confirmation of Publication : 2017. 09. 26
Corresponding Author : Incheol Shin email: ishin@mokpo.ac.kr

the system operation with the availability. This study proposes a novel security framework for the Smart Grid systems to support the availability with priority based on three ideas, identifying abnormal behaviors by the community structure approach, estimating the adversarial impacts on the system from the breaches by the attack tree model and isolating/reporting the attacks by critical point detection technique. With those ideas, we would be able to detect the malicious activities and maintain the overall operation or performance of the systems that the control systems demand during the critical operations on the generation, transmission and distribution of the electricity.

The section 2 provides the literatures on previous studies on abnormal behavior detection in the Smart Grid by highlighting the problems or limits with them, and the next section addresses the structure of Smart Grid with the concept of abnormal behaviors to detect from this study. The section 4 describes our security framework of abnormal behavior detection architecture to support the availability in the Smart Grid systems. Section 5 concludes our study in this paper.

II. RELATED WORK

There have been lots of devotion in the research of abnormal detection systems for the internet systems and, as the advent of Smart Grid, the new design of the detection approaches should be necessitated for different security requirements than the Internet. However, a few number of studies have addressed the issue of the different approaches required to design the security systems for the Smart Grid against cyber-physical attacks.

Isaac Ghansah [1] addressed the security system issues to protect the Smart Grid systems and networks with the differences between the Internet and Smart Grid in terms of the security triad, three core goals of cybersecurity: confidentiality, integrity, availability. The confidentiality is to keep the information in secrete and be accessed by only those who have legally authorized permissions with them. The integrity would be able to guard the information valid and verifiably correct. The availability means that security systems should assure the reliable accesses to the information systems by authorized entities. The study investigates threats, vulnerabilities and risks on the Smart Grid systems with the importance regarding the protection against various cyber-physical attacks in the priority order of the security triad as availability, integrity, credentiality. However, it did not discuss the security system designs to support the ideas with assuring the security triad, AIC.

Furthermore, in accordance with Jess Smith and etc. from [2], only the limitations on the current Intrusion Detection System (IDS) and Intrusion Protection System (IPS) for the Internet has been investigated as applying to the Industrial Control Systems (ICS) systems with the explanation regarding the different security objectives in the control systems from the Internet. That is, the overall security goal from the Internet is to protect the information in the communication networks, but the control systems should keep not only the information data but also the control messages from the various security threats.

R. Bala Sri Swetha and K. Goklia Meena in [3] investigate signature based IDS models with the Smart Grid network signatures and Support Vector Machine (SVM) in order to protect the power grids against various cyber-attacks, DDoS attacks, damaging the integrity of configuration, routing and communication traffic, illegitimate network operation, man-in-the-middle attack and so on by placing IDS in several stages of the hierarchical networks. However, this study addresses merely the issues when placing the IDS in the Internet and the Smart Grid with identification of its appropriate placement in the Smart Grid networks, HAN (Home Area Network), NAN (Neighborhood Area Network) and WAN (Wide Area Network). The appropriate or effective designs of IDS for the control systems are not discussed by the research as well. Since the Smart Grid systems are consisted with various networks, there have been several literatures recommending the efficient placement or deployment of IDS or IPS on Smart Grid networks in [8] and [9], too.

However, because not only the information data but also the control messages are to be flown through the control networks, the security objectives for the control systems are consequently different from the Internet. That is the reason why the security system designs to protect the Smart Grid should be reconsidered and redesigned to augment the robustness of the system. This paper proposes a new design of the IDS to identify the abnormal

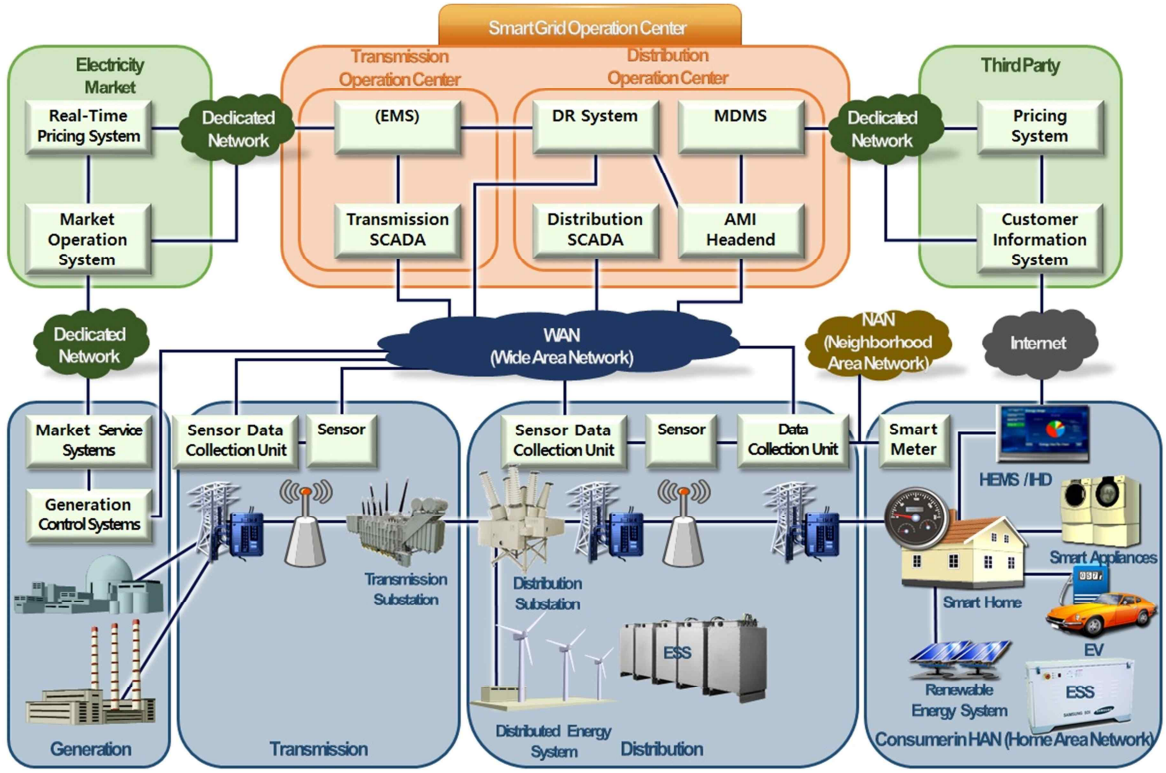

Fig. 1. A Structure of the Smart Grid System

behaviors in the Smart Grid networks.

III. Smart Grid

3.1 Smart Grid System and Applications

The Smart Grid is a new modernized electrical grid to support the efficient energy consumption. The efficiency includes the reliable electricity delivery, more agile outage detection and recovery mechanism, DR (Demand and Response) and so on by employing various two-way communication technologies into existing electrical grids. The communication systems and networks contains various advanced technologies like advanced sensors known as Phasor Measurement Units (PMUs), advanced digital meters called smart meters to report the outages, intelligent substation, automated feeder switches re-routing electrical power around the fault systems etc. Furthermore, electricity consumers would be able to manage their own energy usages with affordable costs by utilizing those systems or services. Fig. 1 depicts the structure and networks of the Smart Grid.

In accordance with Mura Kuzlu etc. in [4] and [5], the networks of the Smart Grid can be represented by a hierarchical multi-layer architecture and classified by data transferring rate and coverage range like below:

• HAN (Home Area Network): The customer area networks with various home and building automation applications related to transmitting/receiving electrical measurement data from various appliances to controllers

• NAN (Neighborhood Area Network): The field areas for smart metering, DR and distribution automation to send various types of messages from many customers/field devices to DCU (Data Collection Unit) and vice versa. The network for this area is to connect the smart meters from HAN to DCU with various communication medium, such as PLC(Power Line Carrier), RF(Radio Frequency), fiber optic cable, twisted pair cable and so on.

• WAN (Wide Area Network): The networks that can allow devices within a large geographic area to communicate with each other for distribution automation and the backbone of the Smart Grid.

3.2 Abnormal Behaviors in the Smart Grid

The electrical power industry has been facing the increasing number of challenges on the processing of

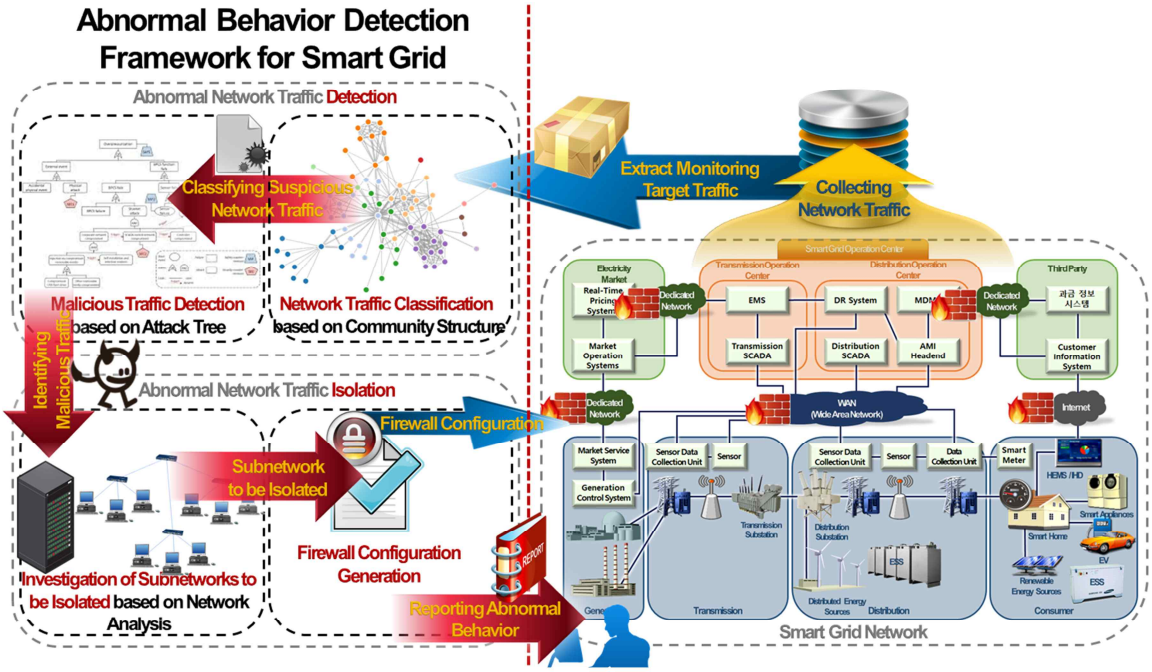

Fig. 2. The Design of the Abnormal Behavior Detection System for the Smart Grid

interconnecting control systems and various types of networks as the deregulation of the electrical market and the trend of convergence with the ICT, the Smart Grid. This advancement helps in moving the outdated, proprietary, closed electrical networks into the more intelligent arena of IT systems.

However, besides gaining all the cost and benefits of IT on the electrical systems, hostile or adversarial activities from the IT would be inherited against them with more lethal damages since the electrical power system is one of the most critical control infrastructures in many nations. A wide range of cyber-attacks to the electrical systems would result in physical performance degradation in various ways since the IT based systems interact or operate the huge number of control systems in the Smart Grid. This has been defined as cyber-physical attacks, and unusual events of network trends in the systems while the continuous monitoring of the systems are addressed as abnormal behaviors, possible threats to the attacks or the attacks themselves.

The mechanism of the Network Behavior Anomaly Detection (DBAD) for the Smart Grid networks is relatively more sophisticated than IT networks because of the type of the messages they carry and the different security triad between them as mentioned before. Since the networks for the electrical power systems deliver both control and information messages, not just like the information only in the IT networks, the DBAD in the Smart Grid should not drop the suspicious or adversarial communication messages after the investigation. However, the impact assessment from the possible security actions to the threats must be conducted before carrying out in order to operate the critical control systems with the availability even under the attacks. In other words, there might be a case of forwarding even suspicious traffic to maintain the operation of the control systems. In this case, the operators should be able to determine the optimal security countermeasures to minimize the impact but maximize the availability of the systems. However, IT based IDS and IPS for the Internet do not need to consider these kinds of operational variety since they exam only information messages in the network traffic.

In accordance with the restrictions and characteristics of the Smart Grid networks, we propose a novel abnormal behavior detection system design for the Smart Grid to support the security triad with appropriate importance order, availability, integrity and credentiality.

IV. Abnormal Behavior Detection Design for the Smart Grid

4.1 Objectives of the Design

In accordance with Lin and Shiping in [10], a large volume of research has been devoted to the

not taken the AIC security triad model, not like CIA triad model in traditional IT system, into account the security measures for the electricity control systems.

Since the traffic in the Smart Grid networks contains not only the information but also the control messages, the security systems in the control systems against the threats should not just simply drop or isolate them from the networks even if they could cause harmful effects on the system. On the other hands, the security systems in IT based communication infrastructures act against the suspicious traffic by removing them out of the networks as quickly as possible because of the CIA in order.

This study proposes a novel security framework, an abnormal behavior detection system, to keep the operational availability of the control systems by considering a unique set of characteristics of the systems. There are three components of sub-security functionalities in this system, extracting the attack vectors from the suspicious traffic in the control networks, assessing the harmful impacts from the threats and finding the optimal points of the networks to perform security actions to minimize the performance degradation or harmful effects on the system. These security sub-functions would be able to keep the soundness of the systems with the availability.

Fig. 2 shows the security framework of abnormal behavior detection system for the Smart Grid in order to support the security triad, availability, integrity and credentiality in order.

4.2 The Design of the Abnormal Behavior Detection Security Framework for Smart Grid

Due to the fact that the existing abnormal behavior detection systems for the Smart Grid have not considered the operational requirement of the appropriate security triad, this study would propose a new security framework design to detect and isolate the malicious traffics to the advanced power grid system while satisfying the requirement of AIC, not CIA in the Internet, by exploring the three key components following.

(1) Discovering Malicious Symptoms from the Networks :

The community structure based network traffic classification is to promptly group the traffic into the sets of communities such that each of them is densely connected internally. This technique from Fig. 3 helps in identifying suspicious communication messages out of them by comparing each group with the existing data set of malicious traffic. Since the investigation on the groups of the traffic would be much faster than each thread of the communication messages, this process reduces the duration of time to extract the malicious activities drastically. In each step of discovering the modules from the graphs, we explore the algorithm for MIEN (Modules Identification in Evolving Network) from Thang N. Dinh in [12].

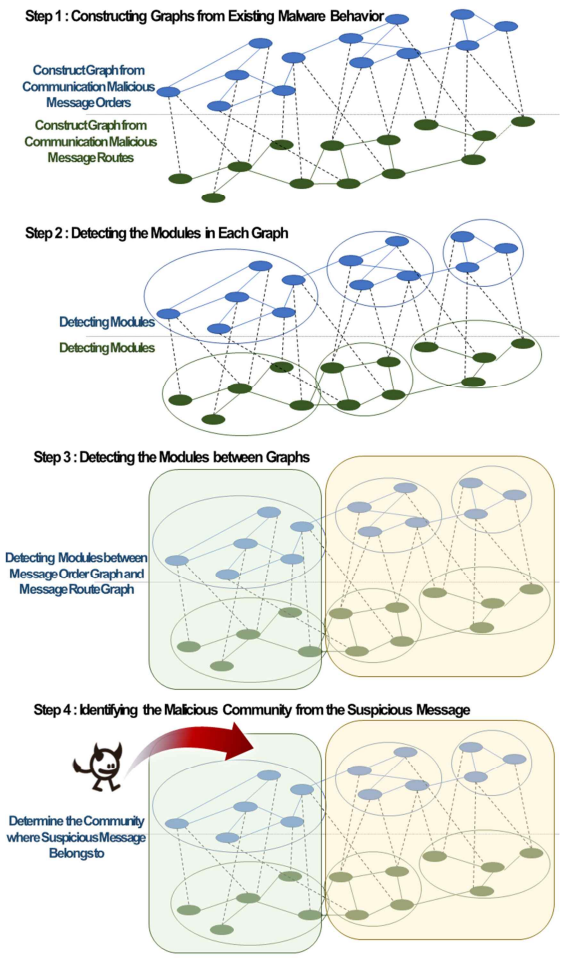

Fig. 3. Description to Identify the Malicious Symptoms from Suspicious Network Messages

In addition, this process reveals the relative distance between the identified malicious data set and collected traffic, which means that it would point out the attacks with different vectors with the same impacts as zero-day attacks as well.

(2) Estimating Security Impacts to the Systems:
After the identification of the malicious community where suspicious network traffic belong to in previous step, the community would provide the pre-studied attacks. Then, we would be able to investigate the impacts from the attacks to the Smart Grid systems. The attack tree based malicious traffic assessment could estimate the impacts from the identified threats on the systems by traversing the attack tree top-down manner. The currently developed attack tree technique has been explored usually in bottom-up manner in order to point out the threats from the attack vectors. However, the security framework for the Smart Grid in our model employs the tree to calculate and investigate the impacts from the identified malicious activities through the previous stage.
This modification of attack tree in the traversing manners would be helpful to estimate the various adversarial effects on the control systems and provide the information for the operators, not security experts but control system managers, to decide appropriate defensive security options while keeping the system operative all the time. This is important since the operators of the Smart Grid are not security experts but highly trained persons to operate the Smart Grid, and they should fully understand on the security status of the systems all the time so as to maintain the system operation based on the malicious impacts from the threats.

(3) Identifying Optimal Points against the Attacks:
The investigation of control restrictions on each subnetworks using Linear Programming (LP) optimization would be able to set up the appropriate network perimeters from spreading the adversarial traffic and minimizing/isolating the impacts on the network. In accordance with Mishra and etc. in [11], there are various types of control networks would be interwoven each other in the Smart Grid, and protocols for the networks interoperate by strict constraints, such as delivery time, length of messages and so on. Consequently, this LP based identification approach would be one of the most efficient approach to find out the optimal points of the networks to perform security actions against the evaluated impacts. The LP is a useful tool to achieve the optimal outcome in a mathematical model whose requirement are represented by linear relations, and the protocol requirements for the Smart Grid could be projected in this manner from the study in [11] and [13].

This study proposes a new security design to detect the various abnormal behaviors from the cyber-physical attacks with the security triad of the Smart Grid by those three steps, extracting malicious symptoms, estimating the adversarial impacts and identifying optimal points to countermeasure.

4.3 Contributions of the Security Framework

This study on designing a novel security framework for Smart Grid shows advantages as following. The first of all, the significance of supporting availability and the design of the adequate security framework for the next generation of power grid systems have been highlighted. Secondly, The security framework for the electrical control systems cannot isolate the suspicious traffic out of the network as soon as the identification like the IT based security systems do because of the security triad order, AIC. In order to support the triad order for the Smart Grid, this work proposes a series of security actions, extracting malicious network traffic, assessing the impact from the threats, pointing out the optimal sub-networks to maintain the operation of the systems. Lastly, how to develop the security systems for the Smart Grid based on the AIC security triad has been introduced by using the three techniques mentioned above.

This work has not conducted the series of experimental simulations since it is hard to find Smart Grid network data, and there has not been research to develop security application like this before. However, as a future work, we will conduct the performance evaluation with comparison to current security systems in the Smart Grid.

V. Conclusion

There have been increasing number of threats from the threat vectors by shifting the legacy electrical systems into advanced power grid systems, the Smart Grid. However, the security technologies have not been considered properly to apply on the

advance electrical power system, but employing existing security methods from the Internet. The important security problem to build the control systems is that it has been proved that the security objective of the advanced electrical control systems is drastically different from the Internet in terms of security triad, AIC not CIA. That is, even though there have been a wide range of research on the Smart Grid security, only a few number of them have been addressing the problem of maximizing or guaranteeing the availability on the Smart Grid yet. Our study has investigated the appropriate design of the security framework to keep the operational availability of the advanced control systems during the protecting them against various cyber-physical threats. There are three technologies has been deployed this security framework, community structure, attack tree, investigation of subnetwork to be isolated.

REFERENCES

[1] Isaac Ghansah (Sacramento, CA, US); David Chambers (Sacramento, CA, US); "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks," Public Interest Energy Research(PIER) Program Project Report

[2] Jess Smith; Nathan Kipp; Dennis Gammel; Tim Watkins (Schweitzer Engineering Laboratories); "Defense-in-Depth Security for Industrial Control Systems," EEA Conference, June, 2016.

[3] R. Bala Sri Swetha; K. Goklia Meena; "Smart Grid – A Network based Intrusino Detection System," International Journal of Computer Applications, International Conference on Innovations in Computing Techniques (ICICT 2015), 2015

[4] The Smart Grid Interoperability Panel Cyber Security Working Group; "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

[5] Murat Kuzlu; Manisa Pipattanasomporn; Saifur Rahman; "Communication Network Requirement for Major Smart Grid Applications in HAN, NAN and WAN," Computer Networks, pp.74-88, 2014

[6] Office of the National Coordinator for Smart Grid Interoperability; "NIST Framework and Roadmap for Smart Grid Interoperability Standards," https://www.nist.gov/sites/default/files/documents/public_affairs/releases/smartgrid_interoperability_final.pdf

[7] ENSIA (European Network and Information Security Agency); "Smart Grid Security," https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf

[8] Thomas M. Overman; Ronald W. Sackman; "High Assurance Smart Grid: Smart Grid Control Systems Communications Architecture," Smart Grid Communications (SmartGridComm), 2010

[9] Chun-Hao Lo ; Nirwan Ansari; "The Progressive Smart Grid System from Both Power and Communications Aspects," IEEE Communications Surveys & Tutorials, vol.14, no.3, pp.799-821, August 2011

[10] Lin Zhou; Shiping Chen; "A Survey of Research on Smart Grid Security," Communications in Computer and Information Science, pp.395-405, 2012

[11] S. Mishra; T. N. Dinh; M. T. Thai; J. Seo; I. Shin; "Optimal Packet Scan Against Malicious Attacks in Smart Grids," Theoretical Computer Science, 2015.

[12] Thang N. Dinh; Incheol Shin; Nhi K. Thai; My T. Thai; "A General Approach for Modules Identification in Evolving Networks, " Springer Optimization and Its Applications, April, 2010

[13] Jin-Bo Kim; Mi-Sun Kim; Jae-Hyun Seo; "Resource management service model implemented for the Internet of Things services access control," Smart Media Journal, Vol.5, No.3, September, 2016

Authors

Incheol Shin
Received the Ph.D. degrees in Computer Engineering from University of Florida in 2010. During 2010-2014, he worked as a Researcher in National Security Research Institute. He is currently an assistant professor at Department of Computer Security in Mokpo National University.