보안공학연구논문지 *Journal of Security Engineering*
Vol.11, No.6 (2014), pp.523-534
http://dx.doi.org/10.14257/jse.2014.12.07

Development of Security Module for Smart Water Meter in the Advanced Metering Infrastructure

Sugwon Hong[1)], Hyung-Mo Park[2)], Soo-Kwon Chae[3)]

Abstract

The Advanced Metering Infrastructure (AMI) is an essential part of the smart water grid. One of the daunting challenges in realizing the services in the AMI system is the security issue. In this paper first we investigate the AMI communication system, and then address security requirements for water meters in the AMI system. We point out the distinguished features of the water meter compared to the smart meter. Then, we address the issues for developing the water meter in three aspects: key distribution, deployment and implementation. Finally, we propose security measures that we take in developing security modules for the smart water meter to meet these requirements.

Keywords : smart water meter, AMI, security, smart water grid

1. Introduction

The Advanced Metering Infrastructure (AMI) is one of the integral components of the smart water grid where water consumption data is collected, stored, and transferred to the utility Meter Data Management System (MDMS). The organizations that are directly involved in promoting and developing the smart water grid have tried to figure out the operating scenarios in the overall domain from water meters up to MDMS, and logical/physical components that should be expected to exist to perform those operations in the full extent. However, how such domain will take shape is still up in the air and requires some time until the actual implementation are in full swing [1].

One of the difficult tasks in realizing the services in this domain is the security issue. While the utility operation system, which is intrinsically the SCADA system, can be almost completely isolated from the outside

Received(November 06, 2014), Review request(November 07, 2014), Review Result(1st: December 15, 2014)
Accepted(December 31, 2014)

[1]449-728 Dept. of Computer Engineering, Myongji Univ., 116 Myongji-ro, Yongin-si, Gyeonggi-do, Korea.
email: swhong@mju.ac.kr
[2]462-120 Passtech Co., Ltd., #1305 Kranz techno, 5442-1 Sangdaewon-dong, Jungwon-gu, Seongnam-si, Gyeonggi-do, Korea
email: passtech@esmartlock.com
[3](Corresponding Author) 461-713 Dept. of Environmental Health and Safety, Eulji Univ., 553 Samseong-daero, Sujeong-gu, Seongnam-si, Gyeongg-do, Korea
email: cskwen@eulji.ac.kr

* This research was supported by a grant (12-TI-C01) from Advanced Water Management Research Program funded by Ministry of Land, Infrastructure and Transport of Korean government.

ISSN: 1738-7531 JSE

world from the communication point, the AMI system will lie in the open domain. Since water meters are located in an open area, any cyber attack that is excruciating service providers and users in the current network could take a toll on the services in the smart grid at the same level [2][3].

In this paper we consider AMI communication systems, and then address security requirements for the smart water meters in the AMI system. Although the requirements are very similar to the ones in the power AMI system, water meters have different features from power meters. We will point out these differences and how these different characteristics might influence developing security mechanisms.

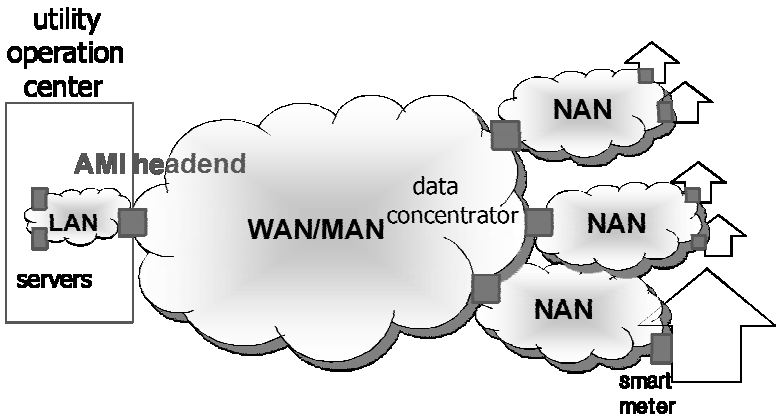
Second, we address development issues of the smart water meter in three aspects: key distribution, deployment issues, and implementation. And then, we show one possible approach we take for developing a security module of the smart water meter.

2. Communication Network

A typical network architecture of the water AMI communication system is shown in [Fig. 1]. Meter Data Management System(MDMS) at the utility operating center collects all data from smart meters at the consumer areas. Meters send data to the nearest concentrator which is called a gateway in this figure and which may be placed on utilities' pole tops. Since they are likely to use wireless communication, a single concentrator can cover a very limited range within which there are approximately no more than several hundreds of water meters. The concentrator sends data to a next level concentrator, making up several stages of traffic concentration until reaching the head-end of a utility operating center, depending on its coverage. Servers placed in the utility side behind the head-end perform various functions based on the collected data. If necessary, they send control/management commands to meters. All the data and command are traversing back and forth through the network.

In the smart grid, three distinct network domains are considered because they have different characteristics and consequently require different communication technologies and network topologies. First, the network domain that consists of in-premise devices and a smart meter is called home area network(HAN). Next, the domain from the smart meters to concentrators is called neighborhood area network(NAN). The last domain from the concentrators and the utility head-end corresponds to wide area network(WAN) in which typical optical fiber SDH or cellular communication technologies are commonly used. In the smart water grid, HAN is unnecessary part since we consider only one device, a water meter, in the customer premise's domain. NAN is contentious part since there is no standard solution so far. For this likely multi-hop wireless network, different proprietary approaches have been considered [4][5][6]. But in order to deploy smart meters and construct networks in compatible way, utility companies and meter vendors realized the standard solution. They worked together in the IEEE 802.15 working group and published IEEE 802.15.4g PHY specification recently for the

utility neighborhood area network, which is also called smart utility networks(SUN) [7]. Even though they still have much work ahead, this effort laid foundation for the deployment of interoperable wireless AMI communication system.



[Fig. 1] The AMI networks

3. Security Requirements

The primary goal of the AMI security is to guarantee secure channels between water meters and a utility head-end. So far, cyber security requirements for the smart grid have been widely studied and several survey papers have been published [2][8][9][10][11]. These works are very comprehensive, and some of the works are not AMI-specific even though they include AMI security as a part of their endeavor,

Unlike the smart meter in the smart grid, we can define the functions of the smart water meter more precisely. Their key functions are real-time monitoring, high-resolution interval metering, and automated data transfer. Sometimes, control servers may issue commands to the water meter for shutting off valves if necessary. Based on these functions of the smart water meter, we can classify security requirements as three categories: data security, physical security, and privacy.

First, the data security concerns achieving secure communication between water meters and the head-end in the utility center, and consequently guarantees data exchange in a secure way. Here, we summarize the essential requirements related to the data security as follows.

Meter authentication: the identity and authenticity of meters and associated customers should be verified before joining the network and receiving proper services.

Message confidentiality: meters should send usage and state information to the head-end securely, and by the

same token the head-end should send commands or other critical information to the meters safely as well. In other words, message contents should be secured not to be read by illegitimate nodes.

Message authentication: receivers need to verify that messages are sent from legitimate senders. Adversaries can forge malicious messages at the either party, consequently causing malfunctions. Meters require strong authentication of the operating servers when they receive any command. On the contrary the server's authentication requirement might be relatively modest. In any case, to verify the owner of messages is one of the most important security requirements in many applications which will take place in the AMI system.

Message integrity and freshness: receivers need to make sure that messages they receive are not altered on the way by adversaries. It is also required that old messages should not be reused by any adversary.

Message non-repudiation: once sending a message, the sender of the message should not deny sending it. This requirement might be necessary for proper billing.

These security requirements can be viewed as a subset of those in the smart meters in the smart grid. But from the point of practical deployment, smart water meters have some different features from smart meters. The most salient point is that power will be supplied to water meters not by power lines but by batteries. Thus, security protocols to meet these requirements for water meters should be energy-sensitive, and for this reason the same protocols which can be applied to the power system might not be feasible in water meters.

Another security requirement noteworthy is physical security [12]. Water meters are more likely to be installed in unmanned and/or unprotected places than their peers in the power system, which implies that they are more vulnerable to physical tampering. Not to mention physical theft and damage, attackers can access firmware data and read stored data, especially recover crypto keys. At worst they can impersonate authorized users to penetrate the grid. Also, the wireless utility network is very vulnerable to physical attack. It is very hard to address this problem. Even so, any physical intrusion to devices should be detectable at least, dispatching warning signals to control nodes as the minimum requirement.

Recently privacy has been emerged as another concern when we provide the AMI services. In the AMI environment usage information may be misused to reveal an individual's personal life style. Someone intentionally peeps others' water usage patterns. In the worst scenario, human behavior at home may lie under surveillance by someone or some organizations [13][14].

4. Challenges

Here, we consider three aspects of security challenges briefly for developing smart water meters to meet the security requirements: key distribution, deployment, and implementation.

4.1 Key distribution

The building blocks of the security protocols are the cryptographic algorithms. Every security protocol is based on the underlying encryption/decryption or hash function keys. Thus, the key management including key establishment is an integral part of the security mechanism. The big picture of the key management in the SCADA security mechanism may be helpful to understand the nature of this challenge [15][16][17][18].

The public key algorithm is generally used as a convenient way in establishing a secure channel for distributing a session key between two network nodes and in authenticating nodes [19]. However, the public key cryptography places computationally heavy burden on the resource-constrained meters. On the other hand, the symmetric key algorithm raises the key management problem in its implementation.

In addition to computational complexity, another important issue to choose the key distribution scheme is scalability [20]. Any key distribution method to be applied to the AMI network should be operated in a large number of meters which have very restricted computing power.

As described in the previous section, the fact that water meters are powered by a built-in battery should be considered when we find the optimum security protocol including key distribution. In this regard a security protocol for smart meters might not be appropriate to apply to smart water meters although both have similar functions and the same security requirements.

4.2 Deployment

Another big challenge in a practical sense is a deployment issue. The AMI in the smart water grid will be built for an extended time and is not able to be installed overnight. As mentioned before, one concentrator will cover approximately hundreds of household meters, and the concentrator will be connected to the ultimate head-end through multiple stage of integration. This tree-like topology may have various forms of network architecture including ad-hoc multi-hop network. In addition to network topology, we have to wait to see which communication technology will be dominant.

There might be discrepancy in space domain as well as time domain. There will be two different space domains which might have incongruous characteristics: residential areas and non-residential areas such as reservoir or water control centers. The latter might be dependent on different communication technology.

Considering these diverse deployment scenarios, we might need dual mode of the key distribution and subsequent data exchange schemes. One is a negotiation-based method. In this scheme either the public key or the pre-installed master keys in the devices can be used at the every handshake stage to setup a session key. The other is free of any negotiation process to setup a session key. Here, a pre-defined key or keys embedded in the device are used session keys without any handshake process between a meter and a server. This scheme

ISSN: 1738-7531 JSE

can obviate any negotiating time, consequently reducing energy consumption because it can send data only when it wants and receives data when it is awake, otherwise it can stay in a sleep mode.

4.3 Implementation

Current water meters basically have two functions: measurement and two-way communication function. For secure communication each meter is also required to have security function on top of them. And they will also have to accommodate some control functions depending on the extent of services that will be provided in the future water grid. These functions should be implemented on an embedded platform that has restricted computing resources. Moreover, the meters will be deployed in unmanned and unprotected location. So they have to be equipped with a certain degree of tamper-proof mechanism. These requirements will restrict the options which we can choose for the security protocol in overall, the key distribution method in particular. To develop meters equipped with those functions with reasonable cost will be one of major practical tasks in developing a security module for the smart water AMI system.

5. Security measures and development

Here, we explain the security measures that we take to meet the security requirements explained in section 3. In our development of the security module for the meter, we concentrate on the data security.

The first thing that we focus on in our implementation is simplicity. The meter has very limited processing capacity, limited memory, and limited power of battery. The battery has to last as long as the meter does, more than 10 years, maybe 15-20 years. Scalability is also very demanding requirement. At the full-fledged deployment the server might have to manage millions of meters. And expandability issue is another important requirement even though this issue is somewhat overlapping with scalability issue. But it is also worth considering when we develope a security module of the water meter because we cannot expect that the deployment would happen overnight, but rather incrementally.

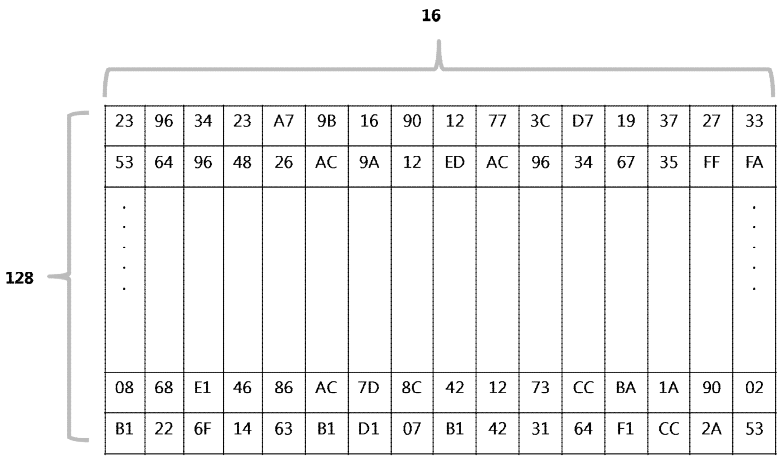
5.1 Trust base

We assume that the security server at the utility operating center is a trusted base, and all meters trust the server at the initial setup. At the deploying time the server and all meters are given the same key table, which contains 128 keys, and the key transformation formula table, which consists of 16 key transformation formulas. The key table is generated by the random number generator, so each meter has a different key table. At the intial registration stage each meter stores these two tables in its EEPROM and keeps them securely thereafter.

Each meter has a unique ID, and at the initial handshake the server authorizes this ID by exchanging an encrypted message. In this way the server verifies authenticity and legality of meters using their meter IDs. Thus, the security protocol is based on the end-to-end model, which means that security responsibility lies on the server and meters, and any security functions are transparent to nodes in the middle. This approach is based on the communication technology in which routing is implemented independently of security function. A different approach is also possible, in which case hop-by-hop authentication is implemented at the nodes of the network [21].

5.2 Key exchange and refreshment

The server and meters use a session key to set up a secure channel between them, and this key is refreshed on a regular base. Each time a meter sends data, it chooses a key from the key table randomly. This key is used as a session key to encrypt data. The meter sends the encrypted data with the key table index.



23	96	34	23	A7	9B	16	90	12	77	3C	D7	19	37	27	33
53	64	96	48	26	AC	9A	12	ED	AC	96	34	67	35	FF	FA
. . . . .															. . . . .
08	68	E1	46	86	AC	7D	8C	42	12	73	CC	BA	1A	90	02
B1	22	6F	14	63	B1	D1	07	B1	42	31	64	F1	CC	2A	53

Ex1: (“16x128 current KEY TABLE” ^ 0x73 & 0x43) & 0xA5
Ex2: (“16x128 current KEY TABLE” >> 0x01 & 0xA5) | 0x31
Ex3: (“16x128 current KEY TABLE” ^ 0x31) + 0x13
[Fig. 2] The example of key table and key table transformation

The session key is ephemeral just as the key table is. The server and meter use a different symmetric key at each data exchange for encryption and decryption. Meters refresh their key tables on a regular base. For refreshing the key table, a meter chooses one of the key transforming formulas in the formula table, which is installed in its memory. The key table refreshment is done by applying this chosen transformation formula to the key table. This operations are based on simple bit operations such as XOR or bit shifting. The examples of

ISSN: 1738-7531 JSE

the key table transformation are shown in [Fig. 2]. Then, the meter sends the chosen index of the transformation formula table to the server. The server also refreshes its key table, stores this information safely, and uses it to select next session key.

In this way, the server and meters can agree a shared key at every data exchange without any hassle. Furthermore, just sending an index of the key transformation formula table can help the server and meters renew a session key every time without involving any complex procedure. A drawback is for meter to have to store the key table of 16 X 128 bytes size and the 16 key transformation table. But it is an affordable burden considering the EEPROM size in our implementation.

For encryption, we use the ARIA algorithm, which has been the Korea Standard block cipher since 2004 [22]. This algorithm is similar to AES algorithm, having the same block size and key sizes. And for a mode of operation we implement the Galois/Counter Mode (GCM) because it performs well in software and is free of intellectual property restrictions. This mode also allows pipelined and paralellized implementations and have minimal computational latency in order to be useful at high data rates [23]. Not only GCM is a mode of operation for block cipher, it also provides data and data origin authentication, which we will explain in the next section.

5.3 Data authentication

For data integrity and sender authenticity, we rely on two methods: ARIA-GCM-128 and the Keyed-Hashing message authentication code(HMAC). We use ARIA-GCM-128 as a default mode because HMAC lengthens the message size, increasing power consumption for cryptographic computation. Our tentative message size is 16 bytes long.

The Galoise/Counter Mode(GCM) is a block cipher mode of operation providing both confidentiality and data origin authentication. GCM has four inputs: a secret key, an initialization vector (IV), a plaintext, and an input for additional authenticated data (AAD). It has two outputs, a ciphertext whose length is identical to the plaintext, and an authentication tag [24].

Data integrity and sender authentication can be also provided by HMAC [25]. In HMAC, the sender A adds a secrete authentication key KAB, which is shared between a sender and a receiver, and the time stamp T to the original data DA, and then computes MAC by applying a hash function to the concatenated data. Next, the sender replaces the secret key with the MAC, and then delivers the data. The complete data that A sends to B is

$$MAC = H(T \mid D_A \mid K_{AB})$$

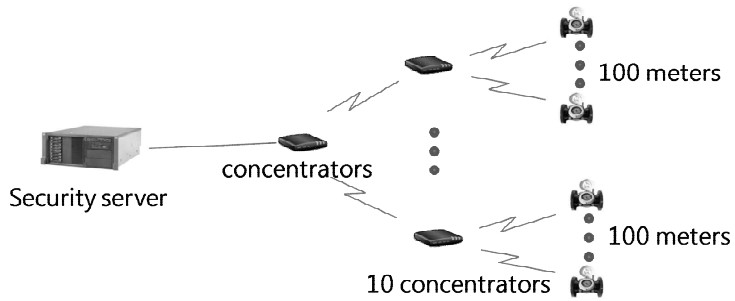
$$A \rightarrow B : \langle T \mid D_A \mid MAC \rangle$$

The secrete key can be of any length. But it is recommended that the key length should not be less than L bytes that is the byte-length of the hash function output, since it would decrease the security strength. Keys longer than L bytes are acceptable but the extra length would not provide significant increase of security [25]. In our implementation we use L=16 as a default secrete key length and use the cipher key for this purpose [26].

The time stamp is used to verify the freshness of the message. Since the time stamp is a non-decreasing number, the value of a new message should be bigger than the one of an old message. Comparing these two values reveals whether the message was resent or not, thus ensuring that no attackers replay old messages.

5.4 Experimental network

Our experimental AMI network consists of two-stage concentration because of its coverage as shown in [Fig. 3]. A concentrator of the first level collects data from 100 meters, and then the second level concentrator collects data from 10 concentrator. In this way, one concentrator communicates 1000 meters within the distance of 2km. Of course, this number is arbitrary. The wireless communication technology we adapted in this experiment network is the IEEE 802.15.4g [7]. This is a standard for the physical layer radio communications required for the utility Neighboring Area Network(NAN). This standard is intended to cover longer range than other 802.15.4 standards. It uses the frequency band of 900MHz in Korea, and data rate is up to 1Mbps, and its coverage is up to 1km.



[Fig. 3] Experimental network

5.5 Development of security module

We develope the security module on the platform of 32bit MCU ARM-based cortex-M3 with 32Kbyte flash memory, 16Kbyte SRAM, and 4Kbyte EEFROM. The specification of the security module is shown in [Table 1]. The key exchange algorithm explained in section 5.2 can be accommodated in this internal memory size, and the whole cipher algorithm, especially ARIA-GCM-128 is implemented on this computing resources.

ISSN: 1738-7531 JSE

As explained in the previous section, the main focus in our development is power consumption. In the smart water meter, power will be supplied not by power lines but by batteries. The battery has to last as long as the meter does more than 10 years. Thus, security protocols to meet these requirements should be energy-sensitive.

The security module processes encryption/decryption of one 16 byte message at 0.04sec with the power consumption of 6.8mA. In order to reduce power consumption we minimize power current during idle state, which is 0.5μA. The overall power consumption depends on other functions of the meter such as communication. So, the frequency of measuring data exchange and the volume of data will also affect power consumption.

[Table 1] security module specification

Classification	Specification
MCU	ultra low power 32bit MCU ARM-based Cortex-M3
power	DC 1.65V to 3.6V power supply
size	l 24mm long, 15mm wide
current consumption	during encryption/decryption : 6.8mA during idle state: 0.5μA
temperature	-20℃ ~ +60℃

6. Conclusion

In this paper we explain the security aspects for developing the smart water meter. We point out different features of the smart water meter compared to the smart meter. And we examine security requirements and propose security measures, taking practical implication into consideration. The security algorithm adapted in developing the security module is based on a simple key management scheme, avoiding complex key management or exchange procedures between a server and a meter. These security measures can be easily expanded to several variants that can be applied to the setup of secure channel between a meter and a server when we deploy smart water meters in the near future.

References

[1] K. Cornish, Addressing the challenges of deploying water AMI, WaterWorld **(2012)**, Vol. 28, Issue 6.

[2] UCAIUG: AMI SEC ASAP , AMI System Security Requirements V1.01, **(2008)**.

[3] S. McLaughlin, D. Podkuiko, and P. McDaniel, Energy theft in the advanced metering infrastructure, Critical Information Infrastructures Security, Lecture Notes in Computer Science **(2010)**, Vol. 6027, pp.176 – 187.

[4] J. Gaoa, Y. Xia, J. Liu, W. Liang, and C. L. Chen, A survey of communication/networking in Smart Grids, Future Generation Computer Systems **(2012)**, Vol. 28, pp. 391 – 404.

[5] J. Zheng, D. W. Gao, and L. Lin, Smart Meters in Smart Grid: An Overview, Proceedings of the IEEE Green Technologies Conference, **(2013)** April 4-5, Denver, USA.

[6] Z. Lipošak1 and M. Boškovi, Survey of Smart Metering Communication Technologies, EuroCon **(2013)**, pp. 1391-1400, Zagreb.

[7] K.-H. Chang, The IEEE 802.15.4g Standard for Smart Metering Utility Networks, IEEE SmartGridComm 2012 Symposium, **(2012)** November 5-8, Tainan City, Taiwan.

[8] The Smart Grid Interoperability Panel – Cyber Security Working Group, Guidelines for smart grid cyber security, NISTIR 7628 **(2010)**, pp. 1 – 597.

[9] W. Wang and L. Zhou, Cyber Security in the Smart Grid: Survey and Challenges. Computer Networks **(2013)**, Vol. 57 , pp. 1344-1371.

[10] A. R. Metke, Security Technology for Smart Grid Networks, IEEE Transactions on Smart Grid **(2010)**, Vol. 1, Issue 1, pp 99-107.

[11] F. M. Cleveland, Cyber security issues for Advanced Metering Infrasttructure(AMI), Proceedings of the IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, **(2008)** July 20-24, Pittsburge, USA.

[12] Power Systems Engineering Research Center, Cyber-Physical Systems Security for Smart Grid, **(2012)**.

[13] NIST, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, NISTIR 7628 **(2010)**.

[14] P. McDaniel and S. McLaughlin, Security and privacy challenges in the smart grid, IEEE Security Privacy **(2009)**, Vol. 7, No. 3, pp. 75 – 77.

[15] L. Pietre-Cambacedes and P. Sitbon, Cryptographic key management for SCADA systems – issues and perspectives, proceedings of the International Conference on Information Security and Assurance **(2008)** April 24-26, Busan Korea.

[16] D. Choi, Advanced Key-Management Architecture for Secure SCADA Communications, IEEE TRANSACTIONS ON POWER DELIVERY **(2009)**, Vol. 24, No. 3, pp. 1154-1163.

[17] N. Liu, , J. Chen, L. Zhu, J. Zhang and Y. He, A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS **(2013)**. VOL. 60, NO. 10, pp. 4746-4756.

[18] S. Das, Y. Ohba, and M. Kanda, S. K. Das, A Key Management Framework for AMI Networks in Smart Grid, IEEE Communications Magazine **(2012)**, August, pp. 30-37.

[19] https://www.certicom.com/images/pdfs/ami/wp-ami-infrastructure-090810.pdf, February **(2009).**

[20] S. W. Smith, CRYPTOGRAPHIC SCALABILITY CHALLENGES IN THE SMART GRID, proceedings of the IEEE PES Conference on Innovative Smart Grid Technologies, **(2012)** January 16-20, Washington DC, USA.

ISSN: 1738-7531 JSE

[21] Yan, Y., Hu R., Das S. Sharif H. and Qian Yi, An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid, IEEE Network, **(2013)** July/August, pp. 64-71.

[22] http://seed.kisa.or.kr/iwt/ko/sup/EgovAriaInfo.do, December **(2004)**.

[23] http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-revised-spec.pdf, May 31 **(2005)**.

[24] J. Viega and D. McGrew, The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP), IETF RFC 4106 **(2005)**.

[25] H. Krawcryk, M. Bellare, and R. Canetti, HMAC: Keyed-Hashing for Message Authentication, RFC 2104, IETF **(1997)**.

[26] I. H. Lim, S. Hong, M. S. Choi, S. J. Lee, T. W. Kim, S. W. Lee and B. N. Ha , Security Protocols Against Cyber Attacks in the Distribution Automation System, IEEE TRANSACTIONS ON POWER DELIVERY **(2010)**, Vol. 25, NO. 1 pp. 448-455.

Authors

Sugwon Hong

1979. 2 : Seoul National University, Physics (BS)

1988. 6 : North Carolina State University, Computer Science (MS)

1992. 6 : North Carolina State University, Computer Science (PhD)

1995. 3 ~ present : Myongji Univ. Dept, of Computer Engineering, Professor

Research Interests : network protocol, network security

Hyung-Mo Park

1985. 2 : Inha University, Dept. of Electronic Engineering (BS)

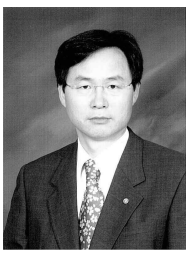
1985. 1 : HANDOK CO., LTD.

1994. 4 : INTEC CO., LTD.

2000. 1 : MOTOROLA/ MSSK(Motorola SmartCard Solution Korea)

2005. 3 ~ present : PASSTECH CO., LTD

Research Interests : Wireless Security, Smart Water Grid Security



Soo-Kwon Chae

1981. 2 : Inha University, Dept. of Civil Engineering (BS)

1985. 2 : Inha University, Dept. of Civil Engineering (MS)

1995. 2 : Inha University, Dept. of Civil Engineering (PhD)

1990. 2 ~ present : Eulji Univ. Dept. of Environmental Health and Safety, Professor

Research Interests : smart water grid, water supply and drainage