SECURITY SCHEMES FOR AMI

Jincheol Kim
KEPCO KDN Co.,Ltd. – Korea
kjc@kdn.com

Seongji Ahn
KEPCO KDN Co.,Ltd. – Korea
sjahn@kdn.com

Youngeok Kim
KEPCO KDN Co.,Ltd. – Korea
yekim@kdn.com

Jongman Kim
KEPCO KDN Co.,Ltd. – Korea
Jmankim@kdn.com

Yunsik Jung
KEPCO KDN Co.,Ltd. – Korea
cys610@kdn.com

Sangjin Kim
KEPCO KDN Co.,Ltd. – Korea
sjkim@kdn.com

ABSTRACT

System and communication protection consists of steps taken to protect the AMI components and the communication links between system components from cyber intrusions. The addition of two way communications between the NAN and the HAN introduces additional risk for unauthorized access to the AMI system. In this paper, we propose new key establishment and security algorithm based on public key encryption to solve AMI network security problems. Also, we evaluate our algorithms performance.

1. INTRODUCTION

The current state of the art in technology and the associated costs are changing rapidly in the area of Advanced Meter Infrastructure (AMI). The direction of these changes may have a dramatic impact on the adoption of AMI and the services that will be available in the near future. AMI smart meters are being offered by a number of vendors. Communication protocols are in flux and no one option has arisen as a global industry standard. In the U.S., Canada, and Europe, several utilities are implementing large AMI projects and their plans for services.

AMI is, therefore, the totality of systems and networks used to measure, collect, store, analyze, and use energy usage data. Smart meters turn into AMI when all the other infrastructure components hardware, software, communications, etc. needed to offer advanced capabilities are added to the smart meter. AMI includes not only the infrastructure from the meter to the utility, but also infrastructure from the meter to the customer that allows the customer to analyze and use the energy data. Also inherent in AMI is the availability of the energy usage data to parties other than the utility to support the provision of energy services or demand response solutions.

Advanced metering infrastructure (AMI) consists of the communications hardware and software and associated system and data management software that creates a two-way network between advanced meters and utility business systems, enabling collection and distribution of information to customers and other parties, such as competitive retail suppliers or the utility itself. AMI provides customers real time (or near real time) pricing of electricity and it can help utilities achieve necessary load reductions.

System and communication protection consists of steps taken to protect the AMI components and the communication links between system components from cyber intrusions. The addition of two way communications between the NAN and the HAN introduces additional risk for unauthorized access to the AMI system. Similarly, the utility NAN, wired or wireless, will offer attackers potential entry points into the network.

For these reasons, compartmentalization of the AMI system and boundary protection should be employed to mitigate risk and limit the impact of unauthorized access to as small of portion of the AMI system as possible. AMI components shall prevent unauthorized or unintended information transfer via shared system resources. The AMI system design and implementation must protect the integrity, the confidentiality, and non-repudiation of electronically communicated information where necessary.

Recent security research for ad hoc networks seemed to focus on distributing the role of the Certifying Authority over some or all devices in the network [1]-[6], the main approach being based on threshold cryptography [7] and allowing specific coalitions of devices to act together as a source of trust such as a certificate authority (e.g., to generate public key certificates). Unfortunately, most of these approaches do not seem to be very efficient, either in terms of computational or communication overhead. Further, even if efficient methods to share trust were available, this only partially solves security issues that may arise in constrained ad hoc networks.

In this paper, we propose new key establishment and security algorithms based on public key encryption to solve AMI network security problems. Also, we evaluate our algorithms performance as followings. First, we establish experiment environment and items, implement our proposed algorithms, and analyze implemented results and experiment result. Section 2 describes AMI network model and Section 3 describes our proposed public key based key establishment and security algorithms. The performance is evaluated in Section 4 via the experiment test. We conclude this paper in Section 5.

2. AMI NETWORK MODEL

The industry and technology surrounding AMI has been evolving at a very fast pace for the past several years. In order to effectively discuss and compare AMI globally, a clear definition of it is required. In some countries, AMI is called smart metering or advanced metering systems (AMS). All these systems describe a method of providing time differentiated information on energy usage to consumers and others. AMI is not a single technology implementation, but rather a fully configured infrastructure that must be integrated into existing and new utility processes and applications. The specification of the infrastructure varies by technology and degree of detail from country to country. The current state of the art of AMI provides us with the following definition.
Generally, an AMI system typically consists of three components: a smart meter at the customer's premise (HAN: House Area Network), a communications network between the smart meter and the utility (SUN: Smart energy Area Network), and a meter data management application (MDM) at the utility. Our AMI Network model is shown as Figure 1. The DCU (Data Collect Unit) is a communication device to collect meter data through sensor network and the ESI (Energy Service Interface) is a communication device to internetwork HAN and SUN through sensor network. However, to be considered as truly AMI, the following capabilities must exist within the system:

- Two-way communication with the meter,
- Home Area Network (HAN) capable,
- Load limiting remote disconnect within the meter,
- Downloadable firmware,
- Capacity to store at least hourly energy reads and collect data daily, and
- MDMS.

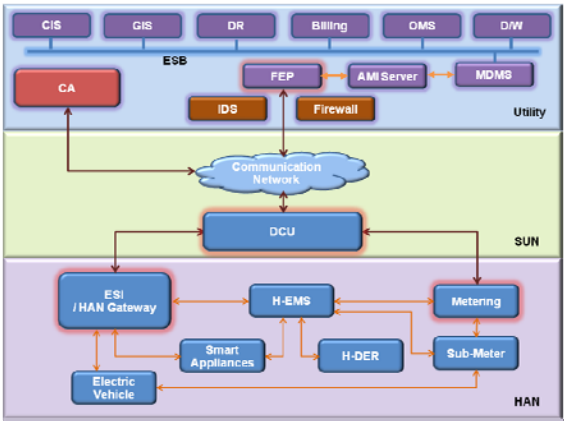

Figure 1. AMI Network Model

3. PROPOSED KEY ESTABLISHMENT AND SECURITY PROCEDURES

In this paper, we propose new key establishment and security procedures to solve AMI SUN/HAN security problems. Our proposed algorithm is composed of four procedures such as key establishment procedure, certificate update procedure, and data encryption procedure.

3.1 Key Establishment Procedure

This procedure is composed of three steps as in Figure 2. Our "Key Establishment Procedure" is public key based key establishment. In [Step1] process, keys and certificates are installed by "Out of band" to meter, DCU, and FEP. Meter is authenticated and received a new encryption key by CA in figure 2. DCU, FEP and ESI are authenticated and received new encryption keys by CA in same process.

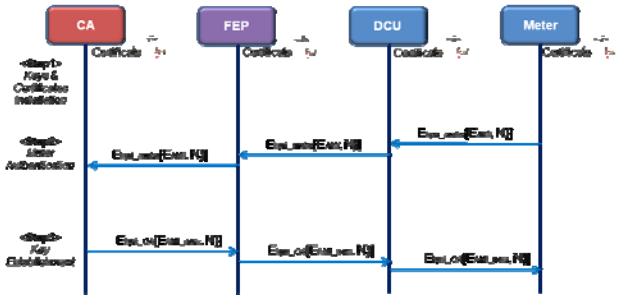

Figure 2. Key Establishment Procedure (Meter)

3.2 Certificate Update Procedure

In this procedure, meter, ESI, and HAN devices update certificates. Meter updates a new certificate and sends a new public key to utility through DCU as in Figure 3.

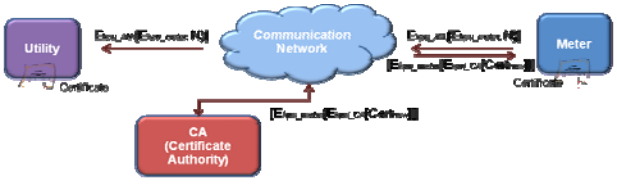

Figure 3. Certificate Update Procedure (Meter)

ESI updates a new certificate and sends a new public key to utility through DCU. Meter and ESI receive new certificates by CA.
HAN devices receive new certificates by ESI in Figure 4. ESI is authenticated by CA in SUN and authenticates HAN devices in HAN.

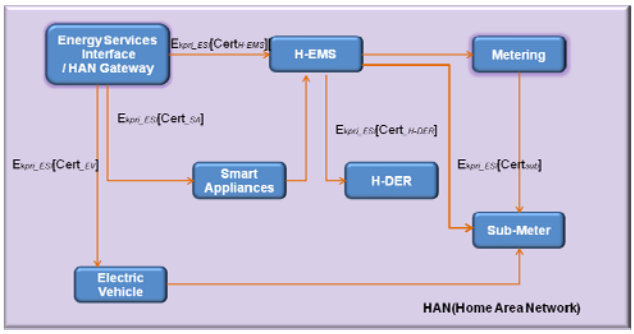

Figure 4. Certificate Update Procedure (HAN)

3.3 Data Encryption Procedure

In this procedure, meter and ESI encrypt data using secret key and public key. Meter and ESI encrypt message, tim e, and hash value using secret key as in Figure 5.

Figure 5. Data Encryption Procedure (Meter)

HAN devices encrypt message, time, and nonce using secret key as in Figure 6.

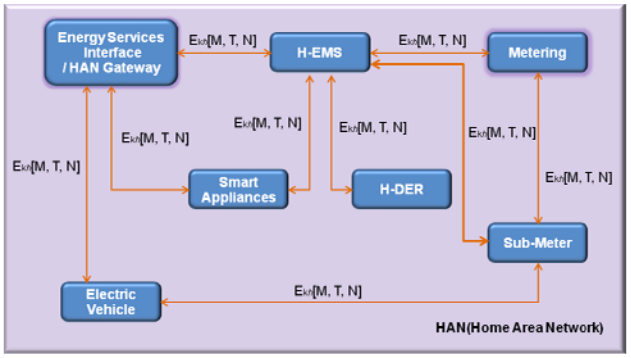

Figure 6. Data Encryption Procedure (HAN)

4. PERFORMACE EVALUATION

In this section, we evaluate the performance of the proposed key establishment and security algorithm to solve security problems of AMI Network. We apply our security algorithms to AMI test bed in KEPCO KDN Kyeonggi branch office. Our test parameter is shown as in Table 1.

Table 1.Test parameter

Items	Values	Remarks
Network Depth	2~3 Hop	
LP Data Size	66Byte	
Fixed Period	232Byte	
Metering Data size		
Key Exchange algorithm	ECC	
Encryption algorithm	AES	
Hash Function	SHA1	

Kyeonggi branch office is four story building, and three smart meters are installed in each floor and total 17 smart meters were installed. Also, three DCUs were installed to 1st floor, 3rd floors, rooftop and test has proceeded present. AMI server collects LP data every 15 minutes, and once a day fixed period metering data. The installed smart meters and DCUs in Kyeonggi branch office are shown in Figure 7.

Figure 7. Installed Smart Meter and DCU

Figure 8 shows that meter communicates with DCU to access SUN and Figure 8b shows that meter communicates with DCU when we apply the security algorithms to AMI test bed.

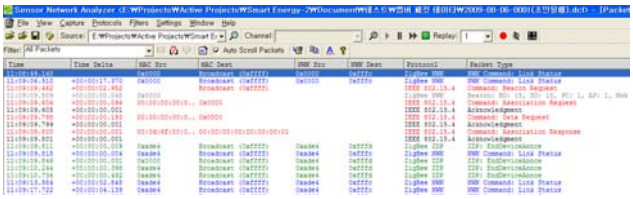

Figure 8a. Protocol Analysis (without Security Procedure)

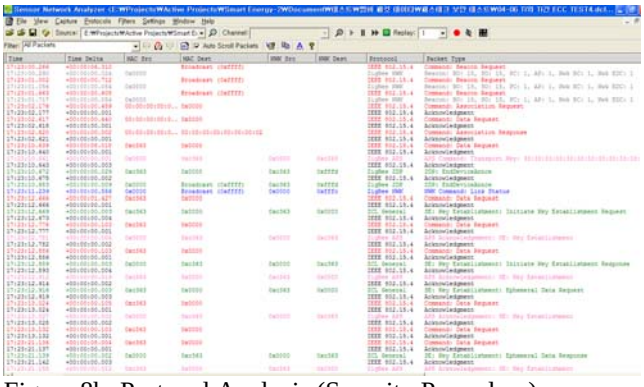

Figure 8b. Protocol Analysis (Security Procedure)

Figure 9 shows the metering rate of effect when we

applied security algorithm to AMI test bed. We applied security algorithm on 1st floor and 2nd floor from December 2, 2010, and applied it on all floors from December 16, 2010, and debugged and applied modified security algorithm from December 28, 2010.

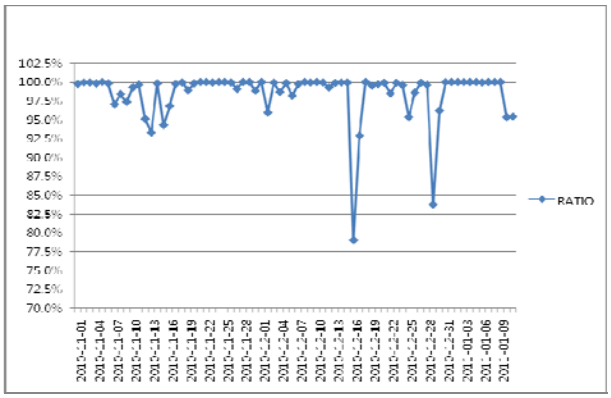

Figure 9. Metering Rate of Effect

5. CONCLUSION

System and communication protection consists of steps taken to protect the AMI components and the communication links between system components from cyber intrusions. The addition of two way communications between the NAN and the HAN introduces additional risk for unauthorized access to the AMI system. Similarly, the utility NAN, wired or wireless, will offer attackers potential entry points into the network.

For these reasons, compartmentalization of the AMI system and boundary protection should be employed to mitigate risk and limit the impact of unauthorized access to as small of portion of the AMI system as possible. AMI components shall prevent unauthorized or unintended information transfer via shared system resources. The AMI system design and implementation must protect the integrity, the confidentiality, and non-repudiation of electronically communicated information where necessary.

In this paper, we propose new key establishment and security algorithms based on public key encryption to solve AMI network security problems. Also, we evaluate our algorithms performance as followings. First, we establish experiment environment and items, implement our proposed algorithms, and analyze implemented results and experiment result.

REFERENCES

[1] L. Zhou and Z. J. Haas, 1999, "Securing Ad Hoc Networks," *IEEE Network Magazine*, vol. 13, no.6, 24-30.

[2] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, 2001, "Providing robust and ubiquitous security support for mobile ad-hoc networks," *Proceedings of International Conference on Network Protocols (ICNP)*

[3] S. Capkun, L. Buttyan, and J.-P. Hubaux, 2003, "Self-organized public-key management for mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, no.1, 52-64.

[4] M. Steiner, G. Tsudik, and M. Waidner, 2000, "Key agreement in Dynamic Peer Groups," *IEEE Trans. on Parallel and Distributed Systems*, vol. 11, no.8, 769-780.

[5] J. Staddon, S. Miner, and M. Franklin, 2002, "Self-Healing Key Distribution with Revocation," *Proc. IEEE Symp. on Security and Privacy (S&P2002)*.

[6] Haiyun Luo, Petros Zefros, Jiejun Kong, Songwu Lu, and Lixia Zhang, 2002, "Self-securing Ad Hoc Wireless Networks," *7th IEEE Symposium on Computers and Communications (ISCC '02.)*

[7] V. Shoup, "Practical Threshold Signatures," 2000, *Advances in Cryptology, EUROCRYPT '00*, 207-220