Paper 0845

## SECURITY SCHEMES FOR AMI

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

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

Yunsik Jung KEPCO KDN Co.,Ltd. – Korea cys610@kdn.com Youngeok Kim KEPCO KDN Co.,Ltd. – Korea yekim@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 twoway 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.

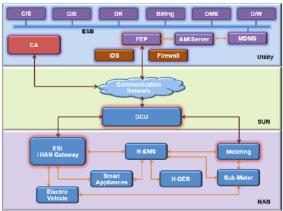


Figure 1. AMI Network Model

#### 3. PROPOSED KEY ESTABLISHMENT AND S ECURITY 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.

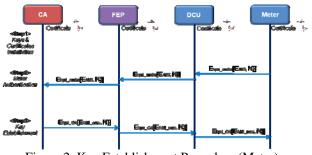


Figure 2. Key Establishment Procedure (Meter)

# 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.

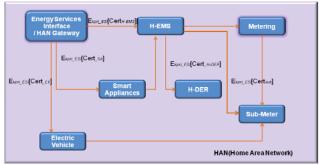


Figure 4. Certificate Update Procedure (HAN)

### **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.

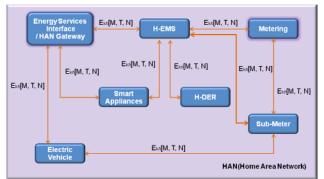


Figure 6. Data Encryption Procedure (HAN)

# 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
		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.

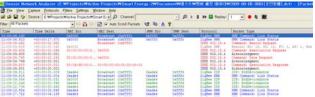


Figure 8a. Protocol Analysis (without Security Procedure)

😂 🖆 🖓 Stautes E-Wholech-WArder Projech-WSmarth + 🔎 Charteel 👘 🖓 🖻 🖬 🕪 🕲 🔡									
ther Al Paciets			R P Arto Scroll Packets	A di ty	7				
Time	Time Delta	NAC Bro	HAC Deat	MMC det	SNOC Dept.	Fratecel	Backet Type		
			Relations control:						
	+00:00100.108	040100				dugbée MMX	Section: BDy 13, 30; 13, 80; 1, Adv 1, Bob 80; 1, Bub 820;		
17:23-01.002	-00100-00.712		Broadcash (Dallit)			1222 012.13.4	Company's Desires Registers		
17122101-064	+00100100.084	0e0000				Zughies HWK	Bearin; 30: 18, 30: 18, 30: 1, 43: 1, 340 80: 1, 840 800;		
17(23)11,043	+05122-04.809		Briedrash (Jeffff)			1222 012.18.4	Contend: Report Report		
	+00+00.00.004	0.0101				Lynes Hay	Bearster SC: 10, 30; 15, 30; 1, AD; 1, 568 SC: 1, 968 SDC:		
	+00:00:00.498	00-00-00-00-00-0	100000			IEEE 905.15.4	Command: Association Report		
17:23:12.177	+00100100.001					IEEE 002.15.4	Arithm/Jedgeett		
17:23:002.417	+50:00:00.440	the bit while the state	Tableh			1EEE 002.15.4	Coment: Data Regulat		
							Advanciatment .		
17133102.620	+10100100.002	Staddadd, Stad	80-10-01-01-00-00-00-00-00-00			1222 022.11.4	Command: Association Response		
17423402.821	+00:00:00.001					IFFE 012.15.4	Advance in the second		
17123123.428	+00100106-117	(+).043	200000			IESE \$12.58.4	Commandol Dalla Regulant		
17:23:10.848	+00100+00.001					TEEE 012.05.4	2/kin/letiment		
17:23:10.643	+55106100.053					TTEE 052.15.4	Arknivladment		
17123110.472	+01100100.029	Cathin	141014	001141	1+1114	Zighes 229	25Ft EntDeviceActors		
17123:10.475	+00100100.002					1257 001.15.4	Acknowledgeent		
17122210,883	+01100100.009	Cattors	Boundsmet clafffft	044343	infffd (	Digles 200	259) Endbwyliahiadw		
17:22:11.230	+00100100.584	0#0000	Broadcast (Saffff)	0x0000	Infffs	States this	INC Command: Ling Status		
17122:12.648	-50100101.421	Ca1543	CATCOL			IEEE 802.15.4	Command: Data Regulat		
17/22/12.668	+00100100.001		and the second s			1222 012.10.4	Arizais/Jedgest		
17(22)12,649	+00100100.005	181543	141110	dac543	Safirit.	hit Seneral	If : Bey Letaplistment: Initiate Boy Intallimpent Report		
17(23)12,473	+00100100.004	(miles)		100.001		1222 212.33.4	Aryung-diment		
17(33(12.178	+90100100-100	Cacial	Testing .			1000 012.18.4	Chesseld) Deta Report		
17123-12.777	+00-00-00.001	0.000	1 Martin 1			TEEE 012.15.4	Acknowledgeent		
	+30,00,00,004	Carling .		Carling	Decree 1	Logice LTS	LPS however, the second second second		
17:23:12.782	+00:00-00.002					IEEE 802.15.4	Acknowledgeent:		
17:23:12.004	+00100100.003	041243	Partners .			CEEE . 802.15.4	Connicd: Data Neguest.		
17123112.004		CRIDED	18.000			INTE 003.15.4	COBRECC: LETE PETLEPT.		
17127012.008	+00100100.003	Capiton .	Taulat .	040100	2442162	tri (mberal	Arkunwisignets 201 New Establishment: Initiate New Establishment Reduction		
27/23:12.883		082535	1001101	58,7123	184,183	ITEE 012.15.4	himsdeinest		
27123132-593	+00100100.008	Card State				2111 902.15.4	Although and a second and a second second second		
		0.000		0.001					
\$7123(32.814	+00+00+00-002	darber .		ductors.	Report 1	ISEE 903.18.4	Address and a second seco		
17:23:12.918 17:23:12.818		081243	1x1110	101210	1.000		Mt Ney Cristiliteent: Sheershi Dels Report		
17122012.018	+00100100.003		Twitted			TETE 052.18.4	Adenteletatent		
17:23:12.124	*90:00:00.509	(ma143	380000				Command: Sets Segment		
17:23:13.124	400+00+00-001					IEEE 012.15.4	Acknowledgeets		
			-341010	040100	Callen .		APS Anything province the day for an income		
17122125.028	+00100100.002					IEEE 812.15.4	Advandedgeett		
17123-13.132	+20100100-503	Cac143	142220			CERE 802.10.4	Commendal Deta Seguent		
17122-12.122	+00100100.001					TEEE 007.58.4	ArknivGeignet8		
17:23:25-534	+00100108-003	044343	101111			IEEE 002.15.4	Consult Data Report		
17:23:21.131	*00:00:00:00					INER 012.15.4	Acknowledgeent		
17:23:21.129	+50:00:00:00+	082000	1er143	0x0100	181143	SUL Owners1	DE: Ney Katellisteent: Epheneral Data Response		
17:23:21.142	+30:00:00.503					ITEE 002.15.4	Acknowledgeent		

Figure 8b. Protocol Analysis (Security Procedure)

Figure 9 shows the metering rate of effect when we

Paper 0845

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.

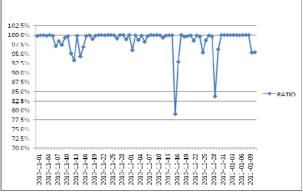


Figure 9. Metering Rate of Effect

### **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

- 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, "Selforganized 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