ACSIJ Advances in Computer Science: an International Journal, Vol. 2, Issue 3, No.4, July 2013
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Security Architecture for Advanced Metering Infrastructure

Seongho Ju[1], Moonsuk Choi[2], Chunghyo Kim[3] and Yonghun Lim[4]

[1] Smart Energy Laboratory, Korea Electric Power Corporation Research Institute
Daejeon, Korea
shju1052@kepco.co.kr

[2] Smart Energy Laboratory, Korea Electric Power Corporation Research Institute
Daejeon, Korea
cms96@kepco.co.kr

[3] Smart Energy Laboratory, Korea Electric Power Corporation Research Institute
Daejeon, Korea
ch2kim@kepco.co.kr

[4] Smart Energy Laboratory, Korea Electric Power Corporation Research Institute
Daejeon, Korea
adsac@kepco.co.kr

Abstract

Advanced Metering Infrastructure (AMI) becomes one of the most realistic and commercial systems in power grid since smart grid has been introduced, but its security issues are not cleared yet because of both economical and technical problems. However, the infringement of privacy becomes under controversy recently, security cannot be an option in deploying AMI system any more. In this paper, we propose the security architecture for AMI system after defining some security requirements, and then the AMI security protocol in more details. The emulation board is implemented in FPGA type to verify that our research is reasonable and realistic.

Keywords: *Authenticated Encryption, Authentication, Key Establishment, AMI, DLMS/COSEM.*

1. Introduction

Power system has evolved toward smart grid based on Information and telecommunication (IT) technology. The activities like international standardization, pilot systems or even construction projects are in full swing in the world, and AMI is at the center of this movement [1]. AMI becomes one of the most realistic and commercial systems in smart grid, and about 600,000 smart meters have already been installed on the spot in Korea. The number of smart meters in the field will be more than ten million until 2016 and reach up to twenty million in 2020 according to KEPCO AMI business plan. However, AMI's security issues are not cleared yet because of both economical and technical problems.

AMI system usually comprises lots of embedded devices like 'data collector', 'communication modem', and 'watt meter' as shown in Fig. 1. They generally have serious limitations in terms of memory and computational power [2] [3] [4]. But more serious problems AMI face is its security. AMI will extend wherever electricity is supplied with tens or hundreds of millions of watt meters, and handle personal information. It must arouse sharp reactions from customers, and the infringement of privacy now becomes under controversy all over the globe [5] [6] [7]. Therefore, security is not an option in AMI system any more, and the security countermeasure against cyber threats should be applied into AMI system somehow.

For this reason, we suggest a security solution for AMI system, and the purpose of this paper is twofold. First, the security architecture will be introduced in chapter 3 after defining some security requirements in chapter 2. Second, the prototype is implemented in FPGA to verify that our solution is reasonable and realistic in chapter 4. We conclude this paper with future works in chapter 5.

2. Requirements

There are two kinds of standpoints considered when the security system is designed for AMI: general security and DLMS/COSEM [8]. The general security requirements in AMI are not much different from ones in typical IT infrastructure which are confidentiality, integrity, device authentication, etc. The latter, DLMS/COSEM, implies its unique characteristic: peer-to-peer communication between DLMS server and client. We derive requirements in the view point of security and DLMS/COSEM in the following subchapters.

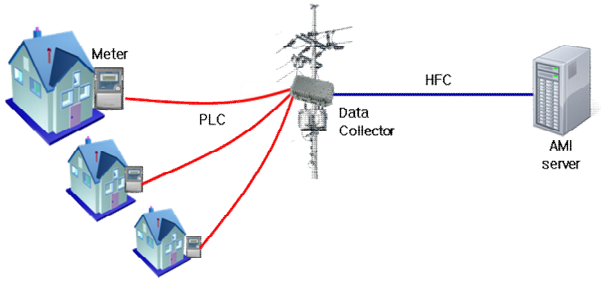

Fig. 1. AMI system in KEPCO

2.1 Security Requirements

AMI security system must be designed considering the items below.

End-to-end security: Because most AMI devices are exposed to outsiders, there are more vulnerable to attacks. Therefore, the communication channel must be virtually set up between meters and an AMI server.

Authenticated encryption: AMI data needs to be protected against both eavesdropping and tampering. It is for privacy protection and exact billing, respectively. It can meet integrity as well as confidentiality of AMI data.

Non-repudiation: Some of AMI data is used for billing services. In this case, not only accurate meter reading but non-repudiation must be supported.

Mutual authentication: All the AMI devices should be able to authenticate each other right after they are installed. This activity may be achieved periodically, of course.

In addition to the conditions mentioned above, more general requirements can be deduced like the followings.

Key management: The secure establishment of encryption keys is as important as, but more difficult to be handled than encryption algorithms. It is a abstruse problem that many researchers try to solve nowadays.

Flexibility & extensibility: The operation span of power system is usually over 10 years, so is AMI. It means that new services can be applied to AMI in the future without any change.

Security strength: Considering the durability of AMI and the advances in IT technology, all the security algorithms should ensure their security strength until they are removed.

Forward secrecy: In case of key leakage, the different keys should be used in each session, and they must not be able to be derived from the exposed key. Various keys are usually created and used for a short term, but the seed key should be stored safely.

Unmanned operation: AMI is normally too large in its scope and volume to be manually controlled. Owing to manpower shortage, most process should go on well automatically.

DLMS User Association suggests standard protocol for metering, and handles how to meet ‘authenticated encryption’ and ‘mutual authentication’ considering ‘security strength’. AES-128 with GCM mode can be a good candidate for AMI security. Unfortunately, there is no specific procedure that utilities or engineering companies comply with, which makes AMI remain unsecure.

2.2 DLMS/COSEM Requirements

DLMS/COSEM is based on server-client model where a watt meter is a DLMS/COSEM server. In AMI, a data collector can be a client to a meter, but not a server to AMI server located in a central data center. It is the reason why two different AMI protocols are used in Korea: one is for communication between meters and data collectors, namely DLMS/COSEM, and another from data collectors to AMI server, KEPCO private protocol. Communication media is the same: Powerline Communication (PLC) between a meter and a data collector, while HFC between a data collector and AMI server as shown in Fig. 1. Under this condition, there are some requirements to be met for AMI security.

Application layer security: A data collector operates as both a protocol converter and media converter between a meter and AMI server. There is no choice except to apply security functions in the DLMS/COSEM application layer regardless of the computing power and memory space of meter. It can also satisfy end-to-end security.

Encryption range: As mentioned above, the protocol conversion is performed in a data collector which gathers data from meters and reassembles the data before sending them to AMI server. Hence, an extra module needs to be introduced to encrypt only the payload of DLMS/COSEM data generated by a meter, but not the header like OBIS code. This duty may be done by a communication modem connected to a meter.

Access control: there are three options for accessing data in DLMS/COSEM: no security, low level security (LLS), and high level security (HLS). Unlike HLS, LLS is a password-based one way authentication, and thus cannot fulfill mutual authentication. Moreover, HLS suggested in

DLMS/COSEM [8] gives us other challenges – what the 'f' function is and how to associate it between a server and a client aside of how to share an encryption key between them.

3. Security Architecture

The AMI security system we designed consists of five sub protocols. The first three protocols in a prerequisite stage are for the mutual authentication, the registration of devices' identification numbers, and key establishment, while the last two are performed during operation.

3.1 Device Authentication

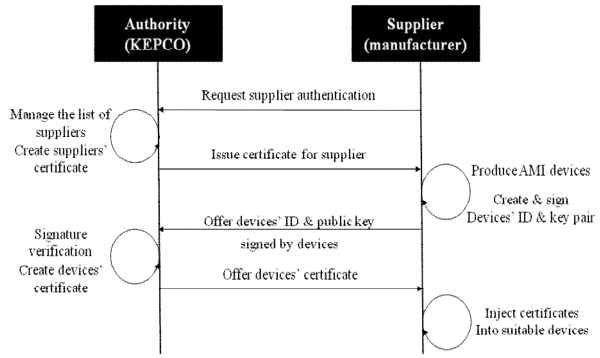

Fig. 2. Authentication prior to delivery

The authentication procedure prior to delivery of goods is done in offline methods (Fig. 2). It does not consume manpower and time, so it is not burdensome. After finishing this procedure, all the devices have AMI server's certificate and their own ones.

3.2 Device Registration

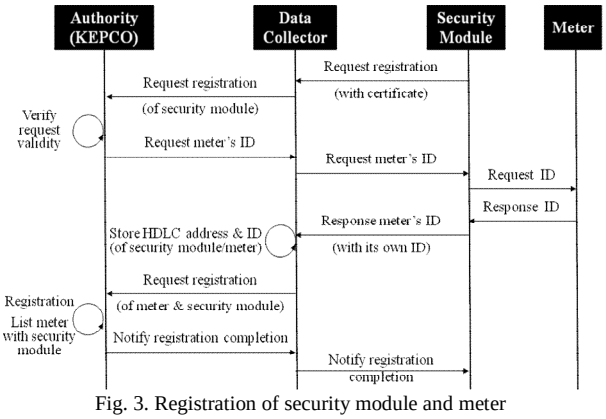

Fig. 3. Registration of security module and meter

This procedure is for verification and registration of meters as well as their security module. We omit the detailed data format and contents, but it is not difficult understanding the flow in Fig. 3. The security module is jointly managed with the meter that it is connected to by an authority (server) and a data collector, and the security module does all the security activity on behalf of its meter from now on.

3.3 Key Establishment

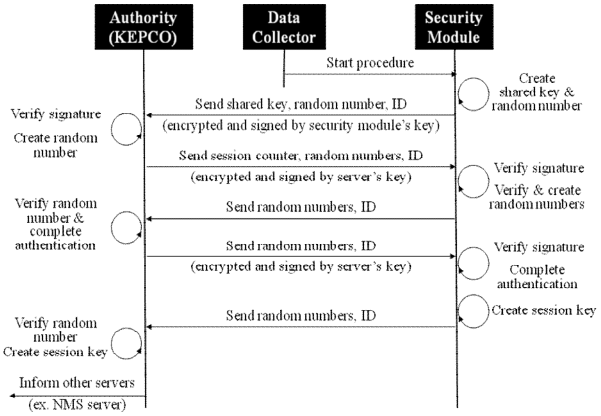

Fig. 4. Key establishment between a security module and authority

The symmetric encryption key is established between a security module and an authority in this step. Like other procedures, key establishment protocol supports end-to-end security, non-repudiation, and mutual authentication. What is more, the session key which will be used to encrypt DLMS/COSEM data is derived from the shared key which must be stored safely and used only to create next session keys. Therefore, the above requirement, forward secrecy' can be met. The procedure for renewal of a session key is the same as this one.

3.4 Secure Meter Reading

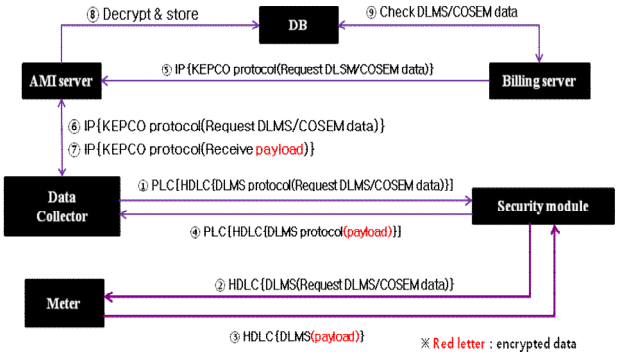

Fig. 5. Workflow of secure meter reading

According to DLMS/COSEM protocol and KEPCO private protocol, a data collector start meter reading and meters are read every 15 minutes. Fig. 5 shows the flow of meter reading, and we indicate encrypted data with red

letter. Following this flow, a data collector does not need to decrypt encrypted data, which meet end-to-end security.

3.5 Certificate Renewal

The certificate is recommended to be refreshed at least every 6 months [7]. We define the procedure of certificate renewal as shown in Fig. 6. The security of this procedure is guaranteed based on the security of the previous ones.

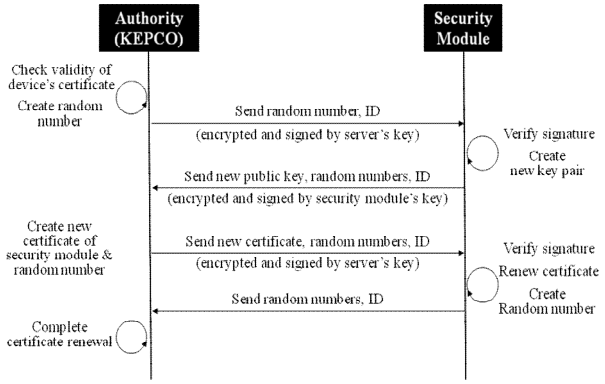

Fig. 6. Renewal of security module's certificate

The security algorithms we adopt are listed in Table 1.

Table 1: Result of FPGA composition

Security Function	Algorithms
Block cipher	ARIA-GCM-128
Hash function	SHA-1
Random number generator	CTR_DRBG(NIST)
Public key encryption	ECIES
Digital signature	EC-KCDSA
Key agreement	ECDH

Block cipher and digital signature algorithms are Korean national standard, and others are international or collective standard. Elliptic curve cryptosystem (ECC) has biggest influence on the performance of security system in general, and 193 bit ECC on binary field is implemented here.

4. Implementation and Test Results

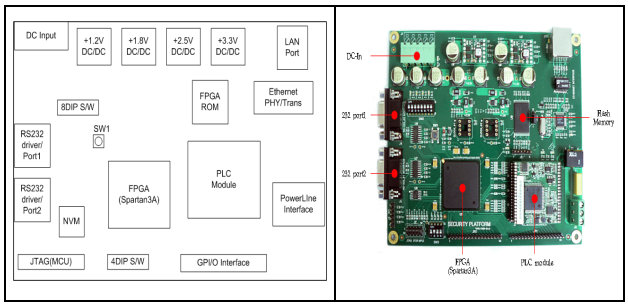

Fig. 7. Block diagram and prototype of security module

The message format is designed in details following the above protocols, but included here on the account of its needlessness and limited space. Instead, we suggest our prototype which emulates the security module and some test results to verify that our research is realistic enough to be applied to AMI system.
The RTL code of the emulation board is composed using Xilinx's FPGA, and the result is in Table 2.

Table 2: Result of FPGA composition

List	Details	Remark
Synthesis Tool	Xilinx ISE10.1 XST	
FPGA Family	Spartan	
Device	Xc3s5000-4fg900	
Top Level Entity Name	AMI security protocol	
Used Slice	30,721 / 33,280	92%
Used Slice Registers	13,797 / 66,560	20%
Used RAMB16s	65 / 104	62%
Operation Frequency	13.5MHz	

The firmware on the board carries out two functions: controlling the process of security hardware engine and handling data according to two AMI protocols (KEPCO private and DLMS/COSEM) and proposed security protocol.

Fig. 8. AMI security testbed

We, first, execute the unit test of the board: data encryption time, signature generation and verification time. The processing time of data encryption time by ARIA is less than 40 μs. Signature generation and verification take about 340ms and 775ms, respectively. The result shows reasonable execution time because it is possible to read meters within 15 minutes if a data collector handles around 200 meters. We also build the testbed which consists of a AMI server, three data collectors, 400 security modules, a meter, and a DLMS emulator as seen in Fig. 8.

The security module is a dedicated MCU where AMI security code is loaded on ARM Cortex-M3 core. A DLMS emulator creates as much data as 400 meters generates and push the data into each security module. One meter connected to a real power load has an interface with a corresponding security module, and push DLMS data into the security module. The result is as follows.

Success rate of meter reading: AMI server could read all the meters within 15 minutes. Data encryption and decryption time was not measured, but the time was included in 15 minutes. We ran the testbed for a week, but no failure was founded.

Success rate of data decryption: AMI server requested retransmission of DLMS data in case of decryption failure and retransmission occurred 5 times out of 672 trials which means that the encryption/decryption failed at a rate of 7%.

Success rate of mutual authentication: In initialization stage, some security modules failed to authenticate with AMI server. It might be caused by all the meters' request at once. However, authentication procedure was completed after a short while, and all the security modules started next steps.

5. Conclusions

In this paper, we show how to secure AMI system. The security requirements for AMI system are deduced, and propose five security protocols from initial authentication to certificate renewal. Our prototype and some test results seem to be reasonable and realistic, so they may be a good guideline for utilities that plan or already deployed AMI.

AMI begins to be deployed in earnest all over the world, but most are without security. Power infrastructure is regarded as a good target to destroy by terrorists. Once AMI is installed on the spot, it will operate for more than ten years. Even now, AMI should be enhanced by proper security functions.

References

[1] F.M.Cleveland, "Cyber security issues for Advanced Metering Infrastructure", in Proc. Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy, IEEE, 2008.
[2] UCAlug: SG Net SRS, "Smart grid networks system requirements specification", 2010.
[3] F.M.Tabrizi, K.Pattabiraman, "A model for security analysis of smart meters", IEEE International Conference on Dependable Systems and Networks Workshops, 2012.
[4] J.Liu, Y.Xiao, S.Li, W.Liang, C.L.P.Chen, "Cyber security and privacy issues in smart grid", IEEE Communications Surveys & Tutorials, vol. 14, no.4, pp.981-997, 2012.
[5] S.R.Rajagopalan, L.Sankar, S.Mohajer, H.V.Poor, "Smart meter privacy: A utility-privacy framework", IEEE International Conference on Smart Grid Communications, pp.190-195, 2011.
[6] A.Cavoukian, K.Kursawe, "Implementing privacy by design: The smart meter case", IEEE International Conference on Smart Grid Engineering, pp.1-8, 2012.
[7] C.Efthymiou, G.Kalogridis, "Smart grid privacy via anonymization of smart metering data", IEEE International Conference on Smart Grid Communications, pp.238-243, 2010.
[8] DLMS UA, "DLMS/COSEM Architecture and Protocols", Green Book 7th edition, 2009.

Seongho Ju received the B.S. degree in electrical engineering from Yonsei University, Seoul, Korea, in 2001, and the M.S. degree in electrical and computer engineering from Seoul National University, Seoul, in 2004. Since he joined Korea Electric Power Cooperation in 2004, he has developed power-line communication, network management system, and especially AMI system as a Senior Researcher. He is a member of WG 15 in TC57, and his recent research areas are in the security system for SCADA, SA, DAS as well as AMI.

Moonsuk Choi received the B.S. degree in electrical wave engineering from Chungnam National University, Chungnam, Korea, in 2003, and the M.S. degree in electronic engineering from Korea Advanced Institute of Science and Technology, Daejeon, in 2005. Since 2005, he has been a researcher with Korea Electric Power Corporation, Korea. His research interests include power-line communication, network management systems, automatic meter reading, and power system security.

Chunghyo Kim received the B.S. degree in electronic engineering from Korea University, Seoul, Korea, in 2003, and the M.S. degree in electronic engineering from Korea Advanced Institute of Science and Technology, Daejeon, in 2005. In 2005, he joined Korea Electric Power Corporation, and he developed Network and System Management (NSM) data object model to monitor and manage power system. His current research focuses on security system for Substation Automation System.

Yonghun Lim received the B.S. and M.S. degrees in electronic engineering from Konkuk University, Seoul, Korea, in 1996 and 1998, respectively. He joined Korea Electric Power Corporation in 1996. He has worked on optic network, wireless sensor network, and radio frequency identification/ubiquitous sensor network as a project leader. His recent research topic is anomaly detection and response in Substation Automation System.