Applied Mathematics & Information Sciences
An International Journal

Mutual Authentication and Key establishment mechanism using DCU certificate in Smart Grid

Soohyun Oh[1] **and Jin Kwak**[2]***[1]**

[1] Department of Information Security Engineering, Hoseo University, Korea
[2] Department of Information Security Engineering, Soonchunhyang University, Korea
Email Address: *shoh@hoseo.edu*

Received: Received May 02, 2011; Revised July 25, 2011; Accepted September 12, 2011
Published online: 1 January 2012

Abstract: The electric power network that used to run as a closed circuit is operated in connection with various wired and wireless networks in the smart grid environment. Thus the security threats in the existing communication environment and additional threats from the characteristics of the smart grid are expected. Therefore, it is critically required to develop of the security mechanism to establish a secure smart grid environment from these threats. In this paper, we propose a mechanism that provides mutual authentication and session key establishment between the smart meter and DCU. The proposed mechanism has advantages in preventing attackers to transmit information, impersonating a smart meter or a DCU, providing confidentiality and integrity to transmitted messages by generating a new key in each session, and management efficiency to use only the DCU's certificate.

Keywords: Smart Grid, Mutual authentication, Key establishment, Public key certificate

1 Introduction

Smart Grid is the next-generation intelligent power grid that maximizes energy efficiency with the convergence of IT technologies and the existing power grid. It enables consumers to check power rates in real time for active power consumption. It also enables suppliers to measure their expected power generation load that stabilizes the operation of the power system.

The communication structure of AMI(Advanced Metering Infrastructure), the core infrastructure to establish a smart grid, consist of intelligent devices, such as smart meter, DCU(Data Concentration Unit) and AMI server. And, power consumption and additional information can be shared between intelligent devices using wired and wireless communication technologies. The electric charges for various consumers, including homes, offices and factories, are readable on a real-time basis so that the power consumption via the shared information can be induced actively. In addition, there are advantages for power service providers to operate more stabilized power systems, since the forecast of the power generation amount is able to be made based on the current power consumption[1]. However, security threats existing in the current communication environment are expected, as well as additional threats caused by the characteristics of the smart grid environment, since the power network, a closed circuit, operates in connecting to various wired and wireless networks[2]. Typical threats include eavesdropping, traffic analysis, intercept/alter, repudiation, integrity violation,

[1] **Corresponding Author: Jin Kwak, jkwak@sch.ac.kr**

masquerade, replay, and malicious code infection. Therefore, it is critically required to develop a security mechanism to establish a smart grid environment secure from these threats.

In this paper, we propose the mechanism in which the mutual authentication and the session key are established between the smart meter and DCU. The proposed mechanism has advantages in preventing attackers to transmit information impersonating as a smart meter or a DCU by mutual authentication between the smart meter and the DCU. The mechanism provides confidentiality and integrity to transmitted messages by generating a brand new key in each session, and management efficiency to use only the DCU's certificate.

2 Related works

2.1 Smart Grid

The communication infrastructure for interworks between the lower level electric systems and the higher level control systems consisting of a smart grid can be established, as shown in Fig. 2.1, with various wired and wireless communication networks[3]. Various communication network technologies including wired network technology, ZigBee technology based on IEEE 802.15, WiFi technology based on IEEE 802.11, Wibro technology based on IEEE 802.16, CDMA based on 3GPP/3GPP2, GRPS, and 3G/4G, can be utilized for its establishment[4].

The AMI communication structure, the major communication infrastructure for interoperation between electric systems and control systems consisting of a smart grid, is divided into three areas, as under[5]:

- *HAN(Home Area Network)*: In the home area of the smart grid, PLC, the communication through power wires and ZigBee, a wireless communication technology for short distance can be used. Also, depending on the place consuming the electricity, BAN(Building Area Network) or IAN(Industry Area Network) are used instead of HAN.
- *FAN(Field Area Network)*: In the field area of a smart grid, wire technologies such as PLC and wireless technologies such as 802.11s Wi-Fi Mesh and IEEE 802.15.4g SUN(Smart Utility Network), and mobile communication technology such as CDMA(Code Division Multiple Access) are used. The network is also referred to as NAN(Neighborhood Area Network).
- *WAN(Wide Area Network)*: The WAN of a smart grid consisted of a core network, MAN(Metro Area Network) and Backhaul network. Cable networks based on Ethernets and often wireless and/or mobile network technology are mostly used for interoperating with the transmission system.

As Fig. 2.2, multiple smart meters connected to one DCU, performing the gateway role in AMI communication environment. Multiple DCUs are also connected to the power service provider's AMI server, forming a multi-layered communication structure.

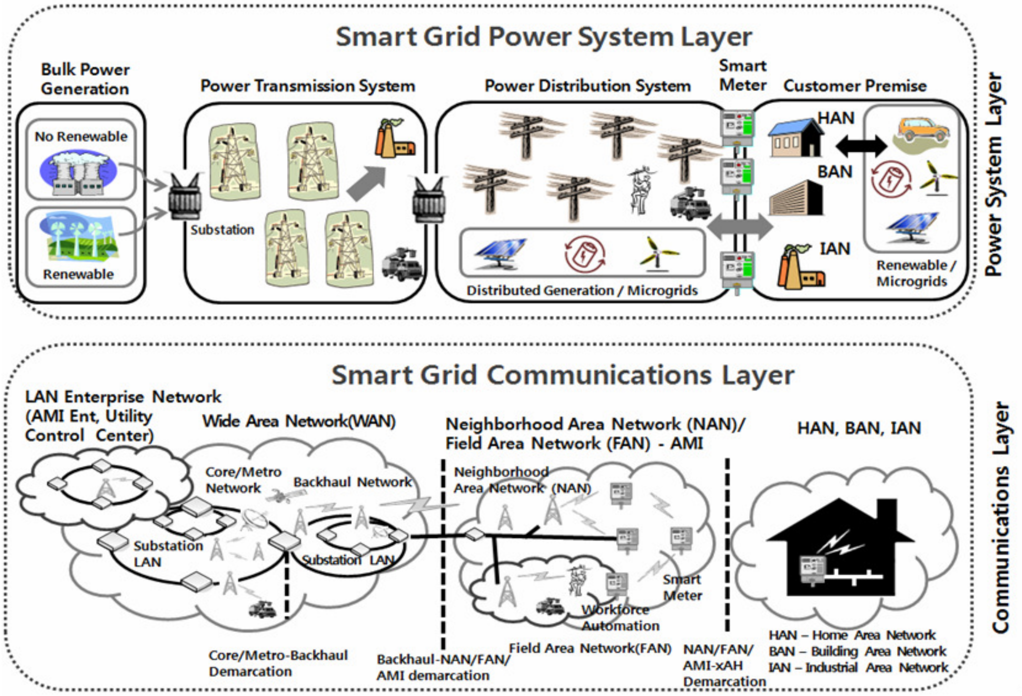
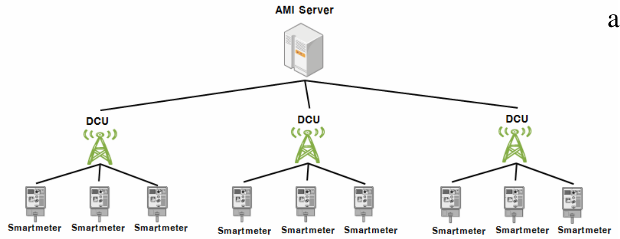

Smart Grid Power System Layer
Bulk Power Generation
No Renewable
Renewable
Power Transmission System
Substation
Power Distribution System
Distributed Generation / Microgrids
Smart Meter
Customer Premise
HAN
BAN
IAN
Renewable / Microgrids
Power System Layer
Smart Grid Communications Layer
LAN Enterprise Network (AMI Ent, Utility Control Center)
Wide Area Network(WAN)
Core/Metro Network
Backhaul Network
Substation LAN
Substation LAN
Neighborhood Area Network (NAN)/ Field Area Network (FAN) - AMI
Neighborhood Area Network (NAN)
Smart Meter
Workforce Automation
HAN, BAN, IAN
Core/Metro-Backhaul Demarcation
Backhaul-NAN/FAN/ AMI demarcation
Field Area Network(FAN)
NAN/FAN/ AMI-xAH Demarcation
HAN – Home Area Network
BAN – Building Area Network
IAN – Industrial Area Network
Communications Layer

Fig. 2.1: Smart Grid communications layer

Fig.



2.2: AMI Communications structure

However, the security threats, such as piracy and unauthorized modification of data resided in the existing communication environment, can be introduced to the smart grid environment due to various communication devices and technologies used in AMI communication structure.

The possibilities of additional threats, such as exposure and abuse of private information, are expected due to the characteristics of the smart grid. Moreover, this may lead to a security incident to the electronic system, one of nation's major infrastructure in case of an attack taking advantage of smart grid environment's vulnerability of security. Therefore, the amplitude of the affect is larger than security accidents in existing communication networks. Therefore, security requirements should be analyzed and a security mechanism to satisfy the requirements should be developed to maintain the advantages of smart grids, in which reliable services are provided.

2.2 Authentication mechanism

The existing ID/PW authentication method has the disadvantage of being vulnerable to replay attacks or dictionary attacks because the same passwords are repeatedly used for a certain period and the length of passwords are relatively short. Therefore, challenge-response authentication method or authentication servers based on tickets are widely used to resolve the problems. In this section, describes the typical challenge-response authentication method and a method using ticket based authentication servers.

(1) Challenge-response mechanism

ISO (International Organization for Standardization) and IEC(International Electrotechnical Commission) have standardized the three challenge-response mechanisms introduced so far as the basic constructs for unilateral entity authentication mechanisms. First, the standardization for mechanism using symmetric cryptographic technique is the called "*ISO Two-Pass Unilateral Authentication Protocol*". It works as follows[6]:

① Bob → Alice : N_B

② Alice → Bob : $E_K(M, N_B)$

③ Bob decrypts the cipher; he should accept the run if he sees N_B or reject the run otherwise.

Here, the first message transmission is often called Bob's challenge to Alice, and the second message transmission is thereby called Alice's response to Bob. Bob is in the position of an initiator while Alice is in the position of a responder. Second, the standardization mechanism using Cryptographic Check Function is called "*ISO Two-Pass Unilateral Authentication Protocol using a Cryptographic Check Function(CCF)*". It functions as follows[7]:

① Bob → Alice : $R_B \| Text1$

② Alice → Bob : Token*AB*

Here Token*AB* = $Text2 \| f_{KAB}(R_B, Bob, Text2)$; f is a CCF, and is essentially a cryptographic hash function. The use of the CCF here is keyed. Upon receipt of Token*AB*, Bob should reconstruct the keyed CCF using the shared key, his nonce, his identity and Text2; He should accept the run if the reconstructed CCF block is identical to the received block, or reject the run otherwise. In the ISO/IEC specification, Text1 and Text2 are optional fields, ǁ denotes bit string concatenation, and RB is a nonce generated by Bob.

Finally, the standardization for mechanism using public key cryptosystem is called "*ISO Public Key Two-Pass Unilateral Authentication Protocol*". It functions as follows[8]:

① Bob → Alice : $R_B \| Text1$

② Alice → Bob : $Cert_A \|$ Token*AB*

Here Token*AB* = $R_A \| R_B \| Bob \| Text3 \| sig_A(R_A \| R_B \| Bob \| Text2)$; $Cert_A$ is Alice's public key certificate. Upon receipt of Token*AB*, Bob should verify the signature; he should accept the run if the verification passes, or reject the run otherwise.

(2) Authentication Mechanism using AS

The authentication mechanism using an authentication server use a centralized authentication server(AS) for the mutual authentication between server and client and sharing the session key, instead of assigning complicated user authentication functions to each servers. Kerberos developed by MIT is one of the most famous types of this method [9]. In Kerberos, after securing Ticket Granting Ticket (TGT) via the Authentication Server(AS), the TGT is submitted to Ticket Granting Server(TGS) to acquire Session Granting Ticket(SGT) to approach the required server in the network. Then, the authentication is processed by submitting the SGT to the server. The session key for secret communication is established after the authentication process succeeds.

The advantage of using the authentication server is in re-using the ticket received from TGS without the re-authentication process during the effective period while no authentication process in the each server is required. However, it is a burden to operate a separate server to establish the authentication system.

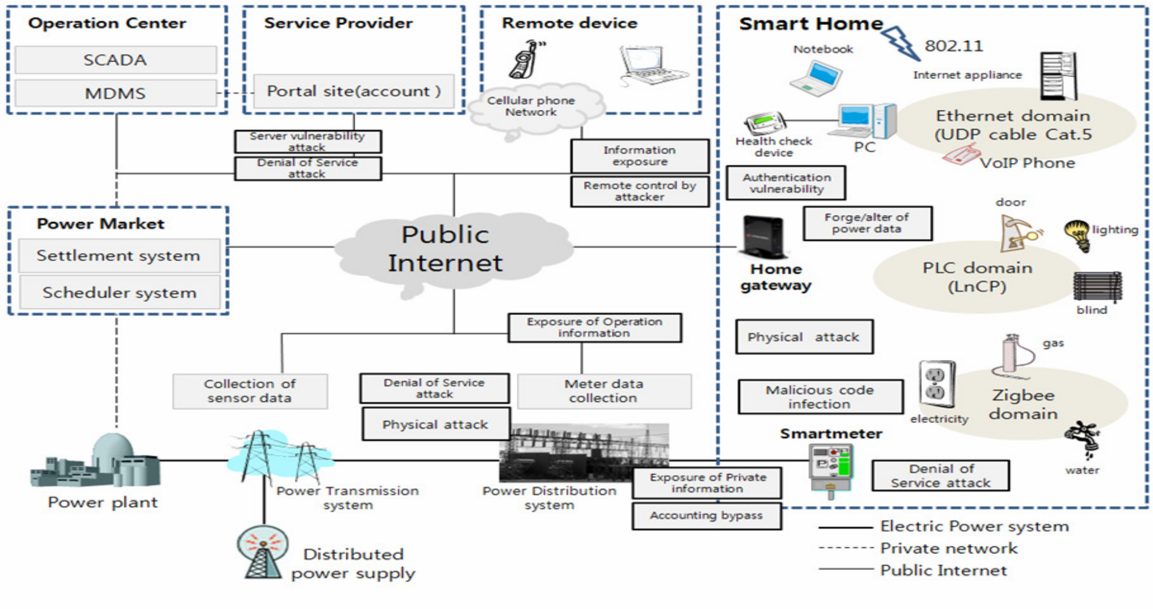


Figure 3.1: Security threats in Smart Grid

3 Security Requirements in the Smart Grid

Security threats in the existing communication environment, as well as the additional threats in the smart grid environment are expected, since AMI technology processes electric power data utilizing communication technology between smart devices. Fig. 3.1 shows the typical security threats that can be shown in the smart grid environments.

A security mechanism satisfying the following security requirements is required to establish a smart grid environment secure from the security threats[10].

- ***Data Confidentiality***: Sensitive information, such as billing and control messages, is transmitted through the network in the smart grid environment. Therefore, the information exchanged in the network should be protected by encryption(s) to prevent it being revealed to an unauthorized third party.
- ***Data Integrity***: Various information such as the power supply meter amount, the information related to charges and the control message, transmitted in the smart grid environment should be protected from forgeries and alterations by illegal or unauthorized accesses.
- ***System Availability***: The availability of devices, systems and networks should be guaranteed to provide stable and continuous bidirectional real-time communication in the smart grid environment.
- ***Mutual Authentication***: An attacker can impersonate himself as a normal user to interrupt the smooth service provided to the users in the smart grid environment. In addition, the attacker can disguise himself as the power service provider to hijack users' private information. An appropriate access control and a mutual authentication mechanism between the each elements of the network should be provided to confront these threats.
- ***Non-repudiation***: A denial prevention mechanism for the messages recorded in the smart meters is required to prevent users' denials on the real-time charge information metered with the smart meter.
- ***Device Integrity***: Smart meters and DCU can be unprotected by personnel and/or other protective measures. Alternatively, the devices

can be installed in vulnerable places to be protected physically. Therefore, protective measures for hardware, software and firmware of devices are critical. If the integrity of the devices is not guaranteed, an attacker can install malicious software in the devices or change the functions of the devices to contaminate the smart grid network or to damage the usability of the smart grid service. Therefore, device integrity verification is required.

- ***Privacy protection***: Information closely related to an individual’s private life can be exposed through information exchanged in the smart grid, such as records, activities and power consumption patterns. Therefore, technical and institutional supplementary devices are required to protect individuals’ privacy.
- ***Light Weighted***: The computation efficiency should be high, since the authentication process should be performed quickly in the smart grid.

Fig. 3.2 shows the correlation between security threat and security requirements[11].

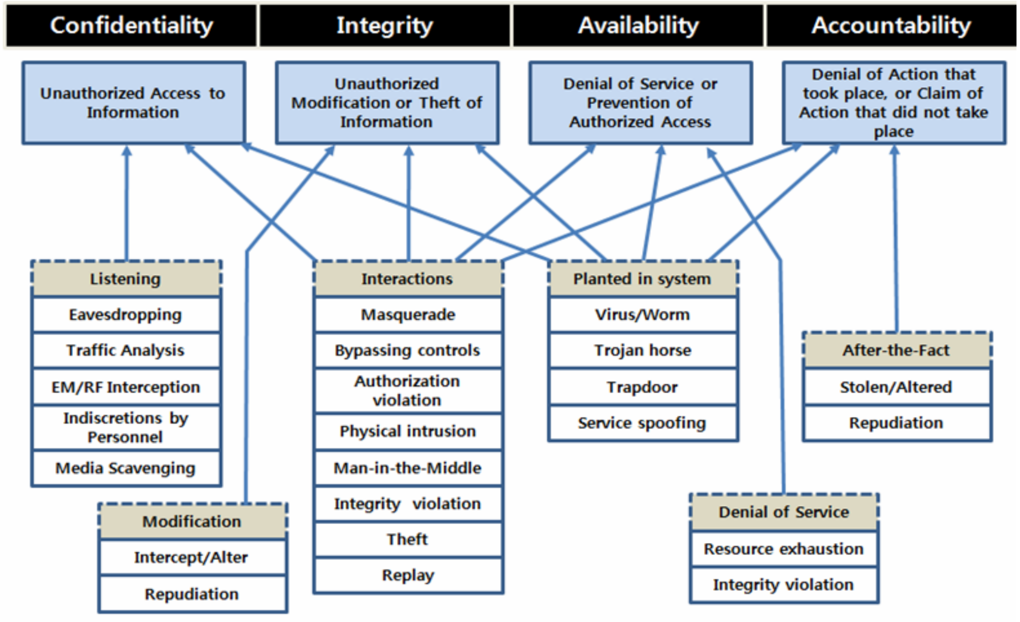


Figure 3.2: Security requirements undermined by security threats

4 The proposed Mutual Authentication and Key Establishment mechanism

A mutual authentication scheme between communicating elements such as the smart meter and the DCU, and the key distribution scheme for secure communication are required to prevent the various security threats possibly happened in the smart grid environment. The challenge-response authentication method described in section 2 has the disadvantage of providing only one-way authentication by which only DCUs can authenticate smart meters while smart meters are not able to authenticate DCUs. The additional key distribution protocol is required to stop the long-term secret key distributed in advance being used continuously for message encryption after completion of the authentication.

In addition, the DCU and all smart meters must have the public key certificates for the mutual authentication in the method using the public key. However, in general, the public key certificate has a valid period; the additional burden to manage certificates of smart meters installed in every home is required. Conversely, it is burdensome to operate additional servers to issue tickets in the method using authentication servers. Therefore, the mechanism is proposed that performs mutual authentication between the DCU and the smart meter using the only DCU’s certificate and generating three new keys used in the current session using the pre-shared long-term key.

4.1 Notations

The notations and their meanings used in the proposed mechanism are:

- MK : Long-term key between Smart meter and DCU
- $Cert_{DCU}$: DCU's public key certificate
- PK_{DCU} : DCU's public key
- $PE_K()$: Encryption function of public key cryptosystem using key K
- $E_K()$ / $D_K()$: Encryption/decryption function of symmetric key cryptosystem using key K
- SK : Session key between smart meter and DCU
- H( ) : Cryptographic hash function
- D_{nonce}/S_{nonce} : a random number generated by DCU/Smart meter
- PRF : Pseudo random function
- MIK : Key used to generate a message integrity value
- TK : Temporal key used to encrypt a message
- KEK : Key encryption key used to encrypt a group key

4.2 The Proposed mechanism

The proposed mutual authentication and key distribution mechanism's operating procedure is:

1) The smart meter transmits the authentication request message to the DCU.
2) The DCU transmits its public key certificate $Cert_{DCU}$.
3) The smart meter verifies the certificate and obtains the DCU's public key.
4) The smart meter generates a random session key SK and encrypts the session key with DCU's public key.
5) The smart meter transmits the encrypted session key to DCU.
6) The DCU decrypts the session key using its own secret key.
7) The DCU generates the random number D_{nonce} and computes the following using the session key and pre-shared MK.

$$H_1 = H(SK, MK, D_{nonce})$$
$$C_1 = ESK(H_1, D_{nonce})$$

8) The DCU transmits C_1 to the smart meter.
9) The smart meter decrypts C_1 and using SK and MK owned by it, checks if the following is satisfied.

$$H_1 ?= H(SK, MK, D_{nonce})$$

10) If 9) is satisfied, the smart meter generates random number S_{nonce} and computes the following using the session key SK and pre-shared MK.

$$H_2 = H(SK, MK, D_{nonce}, S_{nonce})$$
$$C_2 = E_{SK}(H1, D_{nonce}, S_{nonce})$$

11) The smart meter transmits C_2 to DCU.
12) Using the session key SK, D_{nonce} and S_{nonce}, the smart meter computes MIK, TK and KEK as:

$$PRF(SK, D_{nonce}, S_{nonce}) = MIK \parallel TK \parallel KEK$$

13) The DCU decrypts C_2 and using SK and MK owned by it, checks if the following is satisfied.

$$H_2 ?= H(SK, MK, D_{nonce}, S_{nonce})$$

14) If 13) is satisfied, the DCU, using the SK, D_{nonce} and S_{nonce}, computes MIK, TK, KEK as:

$$PRF(SK, D_{nonce}, S_{nonce}) = MIK \parallel TK \parallel KEK$$

15) The DCU encrypts the group key GK using KEK.
16) The DCU transmits the encrypted group key to the smart meter.
17) Using KEK, the smart meter decrypts 16) and obtains the group key GK.

The DCU/smart meter computes the message integrity check value using MIK and encrypts the message using TK for the unicast message transmitted between the smart meter and the DCU, after performing the mutual authentication and key distribution. In contrast, the encryption is performed using GK when the DCU transmits broadcast messages.

5 Analysis

(1) *Mutual authentication and key establishment*

The previously shared long-term secret key MK and the DCU's public key certificate are used to perform the mutual authentication between the DCU and the smart meter in the proposed mechanism. The smart meter encrypts the randomly generated session key SK using DCU's public key and transmits only when the received DCU's

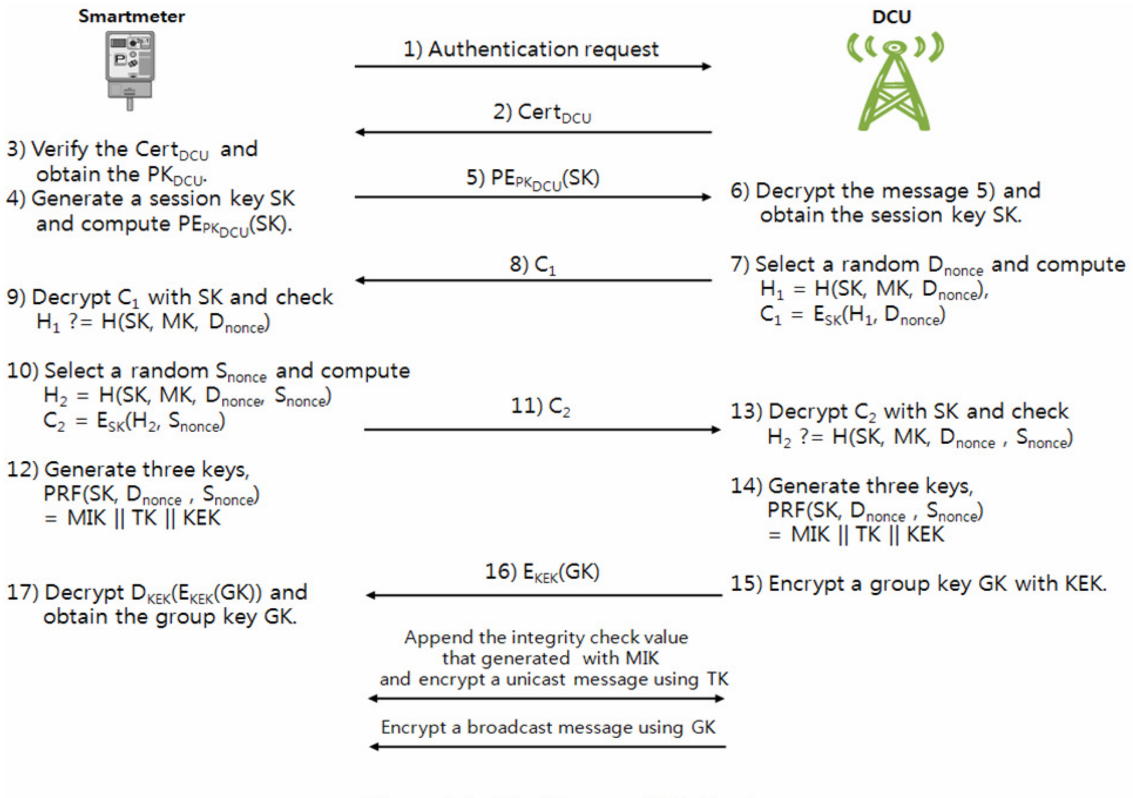

Smartmeter
DCU
1) Authentication request
2) $Cert_{DCU}$
3) Verify the $Cert_{DCU}$ and obtain the PK_{DCU}.
4) Generate a session key SK and compute $PE_{PK_{DCU}}(SK)$.
5) $PE_{PK_{DCU}}(SK)$
6) Decrypt the message 5) and obtain the session key SK.
7) Select a random D_{nonce} and compute $H_1 = H(SK, MK, D_{nonce})$, $C_1 = E_{SK}(H_1, D_{nonce})$
8) C_1
9) Decrypt C_1 with SK and check H_1 ?= $H(SK, MK, D_{nonce})$
10) Select a random S_{nonce} and compute $H_2 = H(SK, MK, D_{nonce}, S_{nonce})$ $C_2 = E_{SK}(H_2, S_{nonce})$
11) C_2
13) Decrypt C_2 with SK and check H_2 ?= $H(SK, MK, D_{nonce}, S_{nonce})$
12) Generate three keys, $PRF(SK, D_{nonce}, S_{nonce})$ = MIK || TK || KEK
14) Generate three keys, $PRF(SK, D_{nonce}, S_{nonce})$ = MIK || TK || KEK
16) $E_{KEK}(GK)$
15) Encrypt a group key GK with KEK.
17) Decrypt $D_{KEK}(E_{KEK}(GK))$ and obtain the group key GK.
Append the integrity check value that generated with MIK and encrypt a unicast message using TK
Encrypt a broadcast message using GK

Figure 4.1: The Proposed Mechanism

certificate is valid. Then, only the legitimate DCU can decrypt the SK using its secret key.

The smart meter can authenticate if the DCU is the correct one acquired by SK and having MK in the procedure 9). The mutual authentication is performed by DCU's verification of the smart meter to be the correct one with the same SK and MK as its own in the procedure 13). Also, the key establishment is performed by generating the message encryption key TK, message integrity check key MIK and the key encryption key KEK using the shared SK and MK between the two devices.

(2) *Key freshness*

The DCU and the smart meter own previously shared long-term key MK in the proposed mechanism. However, it is not desirable to encrypt messages using the same key in every session. Therefore, the DCU and the smart meter respectively generates the message encryption key TK, message integrity key MIK and the key encryption key KEK using MK and newly generated SK, D_{nonce} and S_{nonce} in each session in the proposed mechanism. Therefore, our mechanism provides key freshness.

(3) *Forward secrecy*

When the security of the session key is provided, even if the long-term key is compromised, we states that the forward secrecy is satisfied[12]. In the proposed mechanism, even if the pre-shared key MK between the smart meter and the DCU is compromised, it is infeasible to discover the TK or MIK. Therefore, the proposed mechanism satisfies forward secrecy.

(4) *Man-In-The-Middle attack*

Man-In-The-Middle attack occurs when a hostile attacker enters between two elements conducting mutual authentications and key exchanges and forges/tampers the transmitted messages[13]. In the proposed mechanism, if a attacker replaces the DCU's certificate to his certificate and attempts the man-in-the-middle attack, he can obtain the session key SK generated by the smart meter. However, for the attacker to impersonate himself as the legitimate DCU, he has to compute the ciphertext in the procedure 8). However, the attacker cannot generate the right ciphertext, since he does not know the previously shared MK. Therefore, if an attacker attempts Man-In-The-Middle attack, the attack cannot succeed, in the proposed mechanism, since the smart meter detects false DCUs.

(5) *Efficiency of management*

In the proposed mechanism, only DCU's certificate is used for mutual authentication and key establishment. In general, the method using certificates requires periodical renewal of all certificates, since a certificate has a valid period. However, there is an advantage in terms of certificate management with higher efficiency in the proposed mechanism, since it is not required to install additional certificates in the smart meters located in homes.

6 Conclusion

The electric power network in the smart grid environment, which used to be run as a closed circuit, operates in connection with various wired and wireless networks. Therefore, the security threats in the existing communication environment and additional threats from the characteristics of the smart grid are expected. The typical security threats are eavesdropping, traffic analysis, intercept/alter, repudiation, integrity violation, masquerade, replay and malicious code infection.

In this paper, we proposed the mechanism to establish the mutual authentication and the session keys between the smart meter and the DCU in the smart grid environment. The proposed mechanism can prevent an attacker from transmitting data by impersonating as a smart meter or a DCU transmitting through mutual authentication. The secrecy and the integrity can be provided to transmitted messages by generating a brand new session keys for each session. In addition, the proposed mechanism provides key freshness and forward secrecy and is secure against Man-In-The-Middle attack. Moreover, the proposed mechanism has an advantage in the management, since only DCU's certificates are used.

References

[1] NIST, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0", Sep. 2009

[2] NIST, "DRAFT NIST IR 7628 Smart Grid Cyber Security Strategy and Requirements," Feb. 2010

[3] Claudio Lima, "Smart Grid Communications - Logical Reference Architecture", IEEE P2030-09-0110-00-0011. Oct. 2009

[4] National Energy Technology Laboratory, "Appendix B1: A Systems View of the Modern Grid Integrated Communications," Feb. 2007.

[5] IEEE p2030: http://grouper.ieee.org/groups/scc21/2030/030_index.html

[6] ISO/IEC. Information Technology - Security techniques - Entity Authentication - Part 2: Mechanism using encipherment algorithms. International Organization for Standardization and International Electro-technical Commission, Dec. 1998

[7] ISO/IEC. Information Technology - Security techniques - Entity Authentication - Part 2: Mechanism using a cryptographic check function. International Organization for Standardization and International Electro-technical Commission, Apr. 1998

[8] ISO/IEC. Information Technology - Security techniques - Entity Authentication - Part 2: Mechanism using digital signature techniques. International Organization for Standardization and International Electro-technical Commission, Oct. 1998

[9] RFC 1510, "The Kerberos Network Authentication Service (V5)", 1993

[10] Soohyun Oh and Sunki Eun, "Remote user Access control Mechanism in Smart Grid environments", Transaction of The Korean institute of electrical engineers, Vol. 60, No. 2 Feb. 2011

[11] F.M. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure(AMI)", IEEE, 2008

[12] Wenbo Mao, "Modern Cryptography - Theory and Practice", Prentice Hall, 2004.

[13] Charels P. Pfleeger and Shari Lawrence Pfleeger, " Security in Computing - Fourth edition", Prentice Hall, 2010

Soohyun Oh received her B.S. (1998), M.S. (2000), and Ph.D. (2003) from Sungkyunkwan University (SKKU) in Korea. She is a Professor in the Department of Information Security Engineering, Hoseo University. She is also the dean of the Department of Information Security Engineering. Her research interests include Cryptography, Public key infrastructure, Network security and Smart Grid security. Contact her at shoh@hoseo.edu.

Jin Kwak received his B.S. (2000), M.S. (2003), and Ph.D. (2006) from Sungkyunkwan University (SKKU) in Korea. Prior to joining the faculty at Soonchunhyang University (SCH) in 2007, He joined Kyushu University in Japan as a visiting scholar. Then, he served MIC (Ministry of Information and Communication, Korea) as a Deputy Director. He has served as a Dean of DISE(2009-2010) and Vice-Dean of the College of Engineering (2009) in SCH. He is a Professor in the Department of Information Security Engineering(DISE) at SCH, and is a Director of the SCH BIT Business Incubation Center and a Director of the Industry-University & Institute Partnership Division center at SCH. His main research areas are cryptology, information security applications and information assurance.