International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.3 (2016), pp.411-424
http://dx.doi.org/10.14257/ijmue.2016.11.3.39

Mutual Authentication Scheme Between All AMI Entities in Smart Grid Environment*

Young-Ae Jung

Division of Information Technology Education, Sunmoon University, Korea
dr.youngae.jung@gmail.com

Abstract

These days, most of the important features of advanced metering infrastructure or AMI have already been developed and many AMI devices have been tested in the field as well. However, some security issues still remain unsolved. This paper presents an overview of AMI entities, smart meter, DCU, and MDMS, and then proposes mutual authentication scheme and data exchange schemes between them. More importantly, DCU has not been considered in any authentication scheme until this paper now. The proposed scheme can be adapted easily to the field-testing of the AMI components for enhancing their security.

Keywords: *Security, Mutual Authentication, Smart Grid, AMI*

1. Introduction

As the demand for saving energy increases, managing energy efficiency has also become more important. This has ignited increased interest around the convergence of smart grid and ICT technology. It is possible to exchange two-way information through convergence systems of the existing power network and ICT technology by using the smart grid technology [1]. It has also contributed to improving energy efficiency and developing a new charging service, which considers consumers' requirements and energy consumption pattern by collecting various information rapidly using smart grid. Despite these benefits, smart grid still has a need to be protected from cyber-attacks that occur in such environments where information is exchanged using ICT-based network systems [2-7].

There are various secure authentication schemes in the AMI infrastructure of the smart grid. The AMI infrastructure is composed of home devices, smart meters, DCU (Data Concentration Unit) and MDMS (Metering Data Management System) as shown in Figure 1. However, most proposed authentication schemes have not considered DCU, only composing instead of devices, smart meters, MDMS so far. In the AMI environment, the DCU acts as an intermediary that sends information collected by each smart meter on home devices to the MDMS.

There are many possibilities for the occurrence of security breaches, because the DCU is an important entity with the role of collecting and transferring information. Therefore, it is fundamental to consider a secure DCU authentication scheme in the AMI environment. This paper proposes a secure authentication scheme in order to resolve the security problem mentioned above.

In particular, the proposed scheme puts emphasis on sending messages securely, all along communication areas of the AMI, through mutual authentication between all entities: the smart meter, DCU, and MDMS. Examples of security threats that may arise between the smart meter and the DCU include the occasion of the smart meter sending information to an improper DCU, or the DCU receiving information from fake smart meters with unverified identities.

* This work was supported by the Sun Moon University Research Grant of 2014

ISSN: 1975-0080 IJMUE

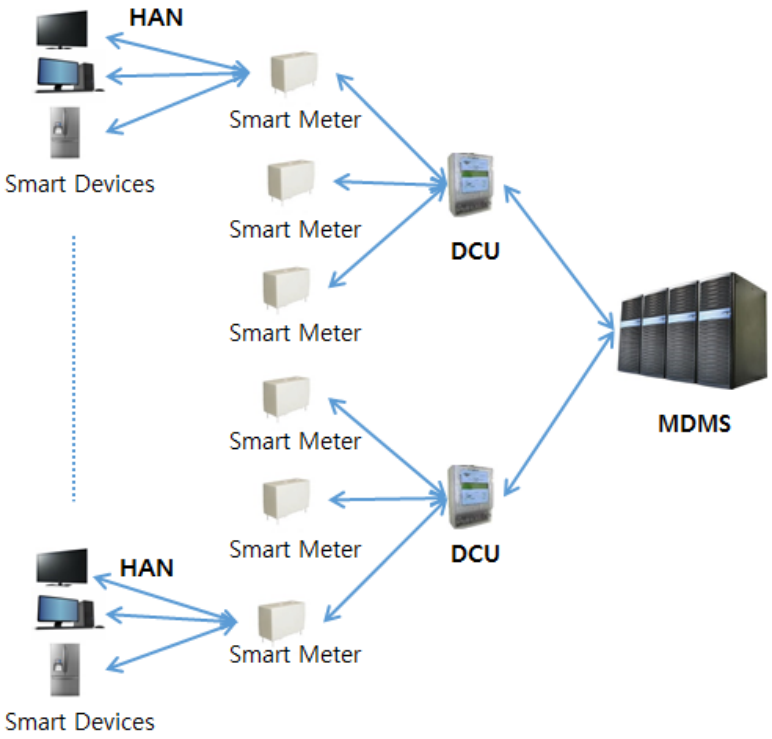

Figure 1. General Architecture of AMI Entities [8]

In order to mitigate security risks that may occur between the smart meter and the DCU, we propose an additional mutual authentication step between the smart meter and the DCU, as a method to address security issues.

This paper contains the introduction in Chapter 1, and covers the related research in Chapter 2. In Chapter 3, this paper proposes the protocol for transmitting metering information securely between the smart meters, the DCUs and MDMS as 6 steps, and describes about the protocol to be performed at each step. Chapter 4 provides the analysis of the proposed security scheme and protocol. Finally, we discuss the conclusion and future research in Chapter 5.

2. Related Work

2.1. AMI Components

As shown in Figure 1, the AMI infrastructure is composed of devices in HAN area, smart meters, DCU that collects metering information produced by each smart meters, and MDMS that transmits data collected by each DCU to the upper level system of power companies [9-10]. Exchanging the indoor information between devices in the AMI environment has performed by using wire or wireless communication. HAN is what they call the technologies for managing communication networks.

PLC (Power Line Communication), ZigBee wireless communication, Ethernet are using for communication in HAN area [11]. The NAN (Neighborhood Area Network) is used between the smart meter, DCU, and MDMS.

2.2. KL Scheme [9]

KL scheme is the method to authenticate and check after generating required information based on the security of N value, which is stored both of device and smart meter after encrypting private N value generated in device [12]. While there is mutual

authentication between a device and a smart meter, the device sends an authentication key to infer random value R, which is included in private value N generated during the registration phase to the smart meter.

This scheme makes the value of P unexposed and infers the value of N. In this scheme, mutual authentication is performed by using P' and V' generated through composing the data and prior information of the device in the smart meter. Non-repudiation is possible while the mutual authentication and data transmission between the smart meter and the MDMS is performing, since the smart meter sends the private key made by using its own MAC address and the private value operated with hash function.

The MDMS receives the encrypted information from the smart meter and sends back its own ID to the smart meter, thereby the smart meter is able to identify the ID of the MDMS and send the metering information to the correct MDMS. Further information on the registration and authentication phase between the device, smart meter and MDMS of KL scheme can be found [9].

2.3. The Vulnerability Analysis of KL Scheme [12]

KL scheme is designed to perform authentication and data transmission between the device and smart meter with the state of fixing private value N to be used in every session. Thus, if there are cases using the public key or the value of N is inferred, a malicious attacker has vulnerabilities about forward security that are able to know the value to be transmitted completely in the session.

Forward security means that malicious attackers are prevented from tracing the confidentiality of past conversations even though they know the present information by succeeding to attack. KL scheme guarantees the security by exchanging the private value of N in the registration phase of device and smart meter. However, if malicious attackers obtain the value of N or symmetric key, they will be able to infer the private value of N. That is, it means that it has the vulnerability to expose the past history, information, and conversation.

2.4. The Vulnerability Analysis of JY Scheme [8]

The JY scheme that was presented in 2015 is very significant in the point of considering the DCU for the first trial in AMI environment. The stability of JY scheme has been increased, by that JY scheme is designed as a security scheme that enables the mutual authentication and key exchange in the AMI environment, considering the DCU for the first time in a domestic area.

The MDMS generates N_{DM} using the private value of the DCU, transmits encrypted information using the key from the DCU, and completes the registration phase. The DCU generates the necessary information for mutual authentication using the received value in the registration phase and transmits it to MDMS.

The MDMS authenticates the DCU using the received information from the DCU, generates other information for authentication and sends it back to the DCU. When the registration and the authentication is performed for both of the smart meter and the MDMS, the DCU, which existed between two sections, doesn't save information generated in the registration phase.

The smart meter generates the metering information encrypted using the key, which makes it possible to encrypt and decrypt only between the smart meter and the MDMS. The smart meter then transmits the double encrypted metering information using the key generated from each the DCU and the MDMS to the MDMS.

3. Mutual Authentication Scheme between All AMI Entities in Smart Grid Environment

3.1. Term Definition

$S : Smart\ Meter$
$D : Data\ Concentration\ Unit$
$M : Meter\ Data\ Management\ System$
$MSG : Metering\ data$
$ID_* : ID\ of\ *$
$R_* : Random\ Number\ of\ *$
$MAC_* : MAC\ Address\ of\ *$
$T_* : Time\ Stamp\ of\ *$
$KS_* : Private\ Key\ of\ *$
$KP_* : Public\ Key\ of\ *$
$K_{*\_*'} : Symmetric\ Key\ between\ *\ and\ *'$
$h(\ ) : Oneway\ hash\ function$
$E(\ ) : Encryption\ function$
$D(\ ) : Decryption\ function$
$\| : Concatenation\ Operation$
$\oplus : XOR\ Operation$

3.2. Mutual Authentication Scheme between All AMI Entities in Smart Grid Environment

The proposed scheme performs a mutual authentication between a smart meter and a DCU, a DCU and a MDMS. A smart meter transmits the generated key K_{S_D} encrypted by the smart meter's public key to the DCU. The DCU generates and stores the secret value X_S encrypted by the DCU's private key. The DCU then generates N by using the MAC address of the DCU and the secret value, and transmits the value encrypted by the symmetric key K_{S_D} of the smart meter to the smart meter. The smart meter gets the secret value and the MAC address of the DCU by decrypting the value received from the DCU, and then the registration phase is completed finally.

A registration phase between the DCU and the MDMS is performed similarly to the registration phase between the smart meter and the DCU. The DCU transmits the generated key K_{D_M} encrypted by the public key of the DCU to the MDMS. The MDMS stores the generated secret value X_D encrypted by the MDMS's private key for the DCU.

The MDMS transmits three values encrypted by the symmetric key of the DCU K_{D_M} to the DCU. The above three values are the MAC address of the MDMS, the time stamps of the MDMS and the N value generated by performing the XOR operation of MAC_D and the secret value X_D. The DCU finishes the registration phase after storing the decrypted two value of MAC_M and X_D from the MDMS.

In the registration phase between a smart meter and an MDMS, the smart meter generates K_{S_M} and transmits K_{S_M}, T_S, MAC_S of the smart meter encrypted by symmetric key KP_M of the MDMS. The MDMS stores MAC_S and K_{S_M} through decrypting transmitted three values.

The MDMS transmits the MAC Address MAC_M and the time stamp T_M of the MDMS encrypted by the symmetric key K_{S_M} of the smart meter. The smart meter finishes the registration phase after storing MAC_S if the time stamp would match the values that are decrypted by the symmetric key. The above three values are the MAC address of the MDMS, the time stamps of the MDMS and the N value generated by performing the XOR operation of MAC_D and the secret value X_D.

Mutual authentication is performed after exchanging keys securely among three devices. Mutual authentication is performed between a smart meter and a DCU, a DCU and a MDMS, a smart meter and a MDMS, and the method of authentication is performed similarly.

For example, the smart meter generates its ID by applying the XOR operation to the random value, the secret value received from the DCU, its MAC address and time stamp, in the mutual authentication phase a smart meter and a DCU. The smart meter generates V that has encrypted the random value, its MAC address and time stamp by using the symmetric key and transmits its ID, V and its MAC address to the DCU.

The DCU checks the MAC address it received by using V and generates W of applying a hash function to R_S, X_S and T_D, if the DCU compares the random value gotten by using the ID of the smart meter and the random vale of the smart meter. After checking the values, the DCU transmits W and its time stamp T_D to the smart meter. The smart meter finishes the authentication phase after comparing the result by performing a hash function to the value received from the DCU with the value generated by itself.

The smart meter makes secret metering data, SM encrypting the real metering data and its timestamp with symmetric key, K_{S_M} and then transmits SM and its MAC address to DCU. The DCU then encrypts SM, MAC_S, T_D using K_{D_M} which is the session key between the DCU and MDMS, and then DCU sends them to MDMS. Finally, MDMS decrypts the real metering data using K_{D_M} and K_{S_M} , and validates all data.

3.2.1. Registration Phase between the Smart Meter and the DCU

Registration phase between the Smart Meter and the DCU procedures are shown in Figure 2.

Figure 2. Registration phase between the Smart Meter and the DCU

(1) The smart meter generates K_{S_D} the value generated by performing the XOR operation of identifier ID_S of the smart meter and a random value R_S and applied a hash function. The smart meter encrypts the symmetric key K_{S_D} between the smart meter and the DCU and the MAC address with the public key of the DCU and transmits to the DCU.

$$\begin{aligned} &\text{Smart Meter: Creates } K_{S\_D} = h(ID_S \oplus R_S) \\ &\text{Smart Meter} \rightarrow \text{DCU: } E(KP_D,\ MAC_S \| K_{S\_D} \| T_S) \end{aligned} \tag{1}$$

(2) The DCU decrypts the message from the smart meter with $\boldsymbol{K_{S\_D}}$ and MAC address of the smart meter MAC_S. The DCU generates and stores the secret value $\boldsymbol{X_S}$ for the smart meter identified ID_S. The DCU encrypts and transmits to the smart meter N generated by performing the XOR operation with MAC_S and X_S, a MAC address of the DCU $\boldsymbol{MAC_D}$ and a time stamps of the DCU $\boldsymbol{T_D}$ with the symmetric key $\boldsymbol{K_{S\_D}}$.

$$\begin{aligned}&\text{DCU: } D(K_{S\_D},\ E\ (KP_D,\ MAC_S \parallel\ K_{\text{S\_D}} \parallel\ T_S))\\&\text{DCU: Creates } X_S \text{ , a secret value for } ID_S\\&\text{DCU: Stores } \ MAC_S, K_{S\_D}, X_S\\&\text{DCU: } N =\ MAC_S \oplus X_S\\&\text{DCU} \rightarrow \text{Smart Meter: } E(K_{S\_D}, N \parallel MAC_D \parallel T_D\ )\end{aligned} \tag{2}$$

(3) The smart meter decrypts the received data from the DCU by using $\boldsymbol{K_{S\_D}}$. The smart meter gets the secret value by performing the XOR operation with N and MAC_S and stores X_S and MAC_D.

$$\begin{aligned}&\text{Smart Meter: } D(K_{S\_D,}\ E(K_{S\_D}, N \parallel MAC_D \parallel T_D)\ )\\&\text{Smart Meter: } X_S\ = N \oplus MAC_S\\&\text{Smart Meter: Stores } X_S,\ MAC_D\end{aligned} \tag{3}$$

3.2.2 Mutual Authentication phase between the Smart Meter and the DCU

Mutual Authentication phase between the Smart Meter and the DCU procedures are shown in Figure 3.

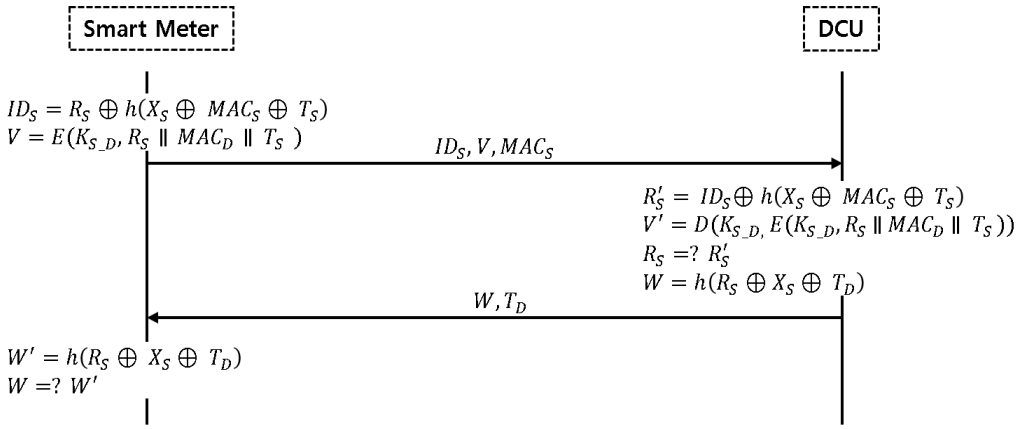

Figure 3. Mutual Authentication phase between the Smart Meter and the DCU

(1) The smart meter generates ID_S by performing the XOR operation with $\boldsymbol{R_S}$ and the result of applying a hash function to X_S, MAC_S and T_S. The smart meter generates the value V that has encrypted R_S, MAC_D and T_S with the symmetric key K_{S_D}. The smart meter transmits ID_s, V and MAC_s to the DCU.

$$\begin{aligned}&\text{Smart Meter: } ID_S = R_S \oplus h\big(X_S \oplus\ MAC_S \oplus\ T_S\big)\\&\text{Smart Meter: } V = E(K_{S\_D},\ R_S \parallel MAC_D \parallel\ T_S\ )\\&\text{Smart Meter} \rightarrow \text{DCU: } ID_S,\ V,\ MAC_S\end{aligned} \tag{4}$$

(2) The DCU decrypts V by the key K_{S_D} gotten by using MAC_S stored in the registration phase. The DCU confirms its MAC address by using the value V. The DCU generates W of applying a hash function to R_S, X_S and T_D, if the random value R_S' gotten by ID_S and R_S are equal. The DCU transmits W and its time stamp T_D to the smart meter.

$$\begin{aligned}&\text{DCU: } R_S' = ID_S \oplus h(X_S \oplus MAC_S \oplus T_S)\\&\text{DCU: } V' = D(K_{S\_D}, E(K_{S\_D}, R_S \parallel MAC_D \parallel T_S))\\&\text{DCU: } R_S =? R_S'\\&\text{DCU: } W = h(R_S \oplus X_S \oplus T_D)\\&\text{DCU} \rightarrow \text{Smart Meter: } W, T_D\end{aligned} \tag{5}$$

(3) The smart meter generates W' of applying a hash function to T_D, R_S and X_S and finishes the authentication after checking whether W' and W are equal or not.

$$\begin{aligned}&\text{Smart Meter: } W' = h(R_S \oplus X_S \oplus T_D)\\&\text{Smart Meter: } W =? W'\end{aligned} \tag{6}$$

3.2.3. Registration phase between the DCU and the MDMS

Registration phase between the DCU and the MDMS procedures are shown in Figure 4.

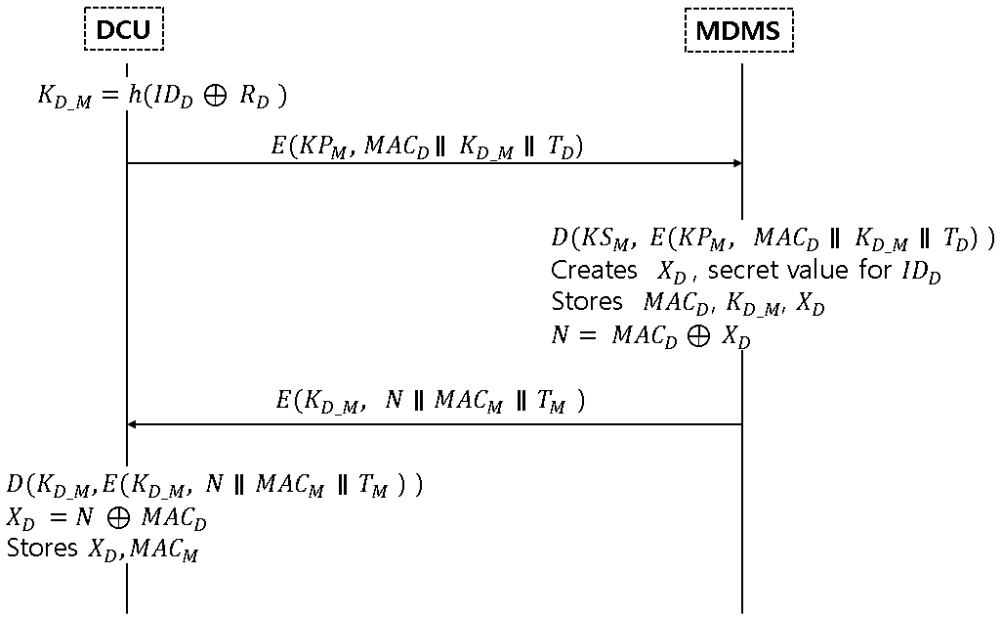

Figure 4. Registration phase between the DCU and the MDMS

(1) The DCU generates K_{D_M} of applying a hash function to the result by performing with ID_D of the DCU identifier and a random value R_D. The DCU encrypts its MAC address MAC_D, K_{D_M} and T_D by the public key KP_M and transmits to the MDMS.

$$\begin{aligned}&\text{DCU: Creates } K_{D\_M} = h(ID_D \oplus R_D)\\&\text{DCU} \rightarrow \text{MDMS: } E(KP_M, MAC_D \parallel K_{D\_M} \parallel T_D)\end{aligned} \tag{7}$$

(2) The MDMS decrypts the value from the DCU by its private key and stores K_{D_M} and MAC_D of a MAC address of the DCU. The MDMS generates and stores the secret value for the DCU. The MDMS generates N by performing the XOR operation with MAC_D and the secret key X_D. The MDMS encrypts N, its MAC_M and T_M by the symmetric key K_{D_M} received from the DCU and transmits it to the DCU.

$$\begin{aligned} &\text{MDMS: } D(KS_M,\ E(KP_M,\ MAC_D \parallel K_{D\_M} \parallel T_D)) \\ &\text{MDMS: Creates } X_D \text{, a secret value for } ID_D \\ &\text{MDMS: Stores } MAC_D, K_{D\_M}, X_D \\ &\text{MDMS: } N = MAC_D \oplus X_D \\ &\text{MDMS} \rightarrow \text{DCU: } E(K_{D\_M},\ N \parallel MAC_M \parallel T_M) \end{aligned} \quad (8)$$

(3) The DCU decrypts the message from the MDMS by the symmetric key K_{D_M} and stores MAC_M. The DCU generates and stores X_D by performing the XOR operation with N and MAC_D.

$$\begin{aligned} &\text{DCU: } D(K_{D\_M},\ E(K_{D\_M},\ N \parallel MAC_M \parallel T_M)) \\ &\text{DCU: } X_D = N \oplus MAC_D \\ &\text{DCU: Stores } X_D,\ MAC_M \end{aligned} \quad (9)$$

3.2.4. Mutual Authentication phase between the DCU and the MDMS

Mutual Authentication phase between the DCU and the MDMS procedures are shown in Figure 5.

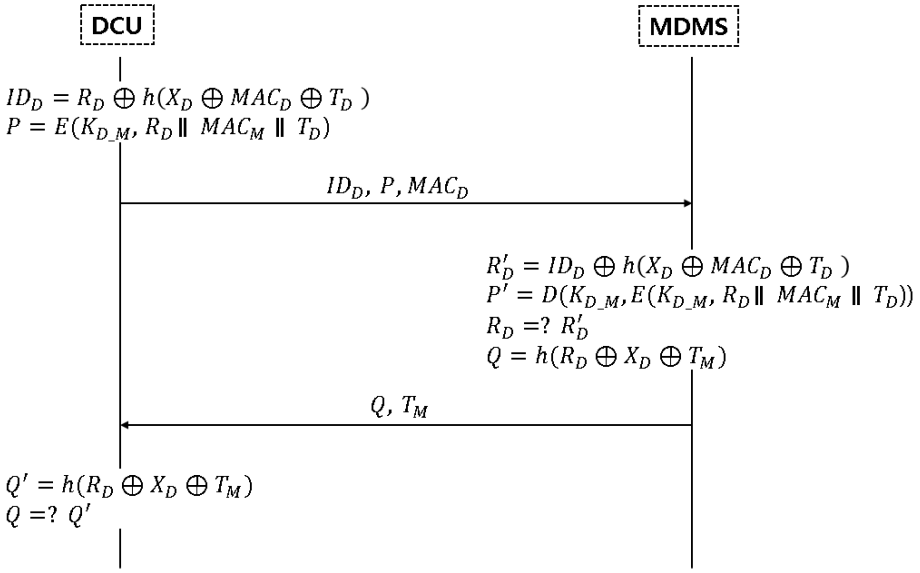

Figure 5. Mutual Authentication Phase between the DCU and the MDMS

(1) The DCU generates ID_D by performing the XOR operation with $\boldsymbol{R}_D$ and the result of applying a hash function to X_D, MAC_D and T_D. The DCU generates the value that has encrypted R_D, MAC_M and T_D with the symmetric key K_{D_M}. The DCU transmits ID_D, P and MAC_D to the MDMS.

$$\text{DCU: } ID_D = R_D \oplus h(X_D \oplus MAC_D \oplus T_D)$$

$$\begin{aligned} &\text{DCU: } P = E(K_{D\_M},\ R_D \parallel MAC_M \parallel T_D) \\ &\text{DCU} \rightarrow \text{MDMS: } ID_D,\ P,\ MAC_D \end{aligned} \tag{10}$$

(2) The MDMS decrypts P by the key K_{D_M} gotten by using MAC_D stored in the registration phase. The MDMS confirms its MAC address by using the value P. The MDMS generates Q of applying a hash function to R_D, X_D and T_M, if the random value R_D' gotten by ID_D and R_D are equal. The MDMS transmits Q and its time stamp T_M to the DCU.

$$\begin{aligned} &\text{MDMS: } R_D' = ID_D \oplus h(X_D \oplus MAC_D \oplus T_D) \\ &\text{MDMS: } P' = D(K_{D\_M}, E(K_{D\_M},\ R_D \parallel MAC_M \parallel T_D)) \\ &\text{MDMS: } R_D =?\ R_D' \\ &\text{MDMS: } Q = h(R_D \oplus X_D \oplus T_M) \\ &\text{MDMS} \rightarrow \text{DCU: } Q, T_M \end{aligned} \tag{11}$$

(3) The DCU generates Q' of applying a hash function to T_M, R_D and X_D and finishes the authentication after checking whether Q' and Q received from the MDMS are equal or not.

$$\begin{aligned} &\text{DCU: } Q' = h(R_D \oplus X_D \oplus T_M) \\ &\text{DCU: } Q' = Q \end{aligned} \tag{12}$$

3.2.5. Registration phase between the Smart Meter and MDMS

Registration phase between the Smart Meter and MDMS procedures are shown in Figure 6.

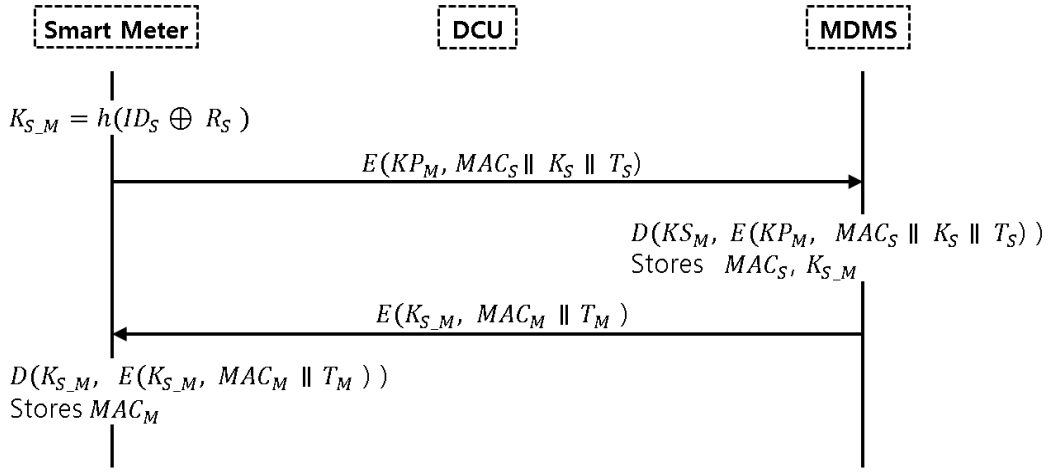

Figure 6. Registration phase between the Smart Meter and MDMS

(1) The smart meter generates K_{S_M} of applying a hash function to the result by performing with ID_S of the smart meter identifier and a random value R_S. The smart meter encrypts MAC_S, , K_S and T_S by the public key KP_M and transmits to the MDMS.

$$\begin{aligned} &\text{Smart Meter: } K_{S\_M} = h(ID_S \oplus R_S) \\ &\text{Smart Meter} \rightarrow \text{MDMS: } E(KP_M,\ MAC_S \parallel K_S \parallel T_S) \end{aligned} \tag{13}$$

(2) The MDMS decrypts the message from the smart meter by its private key and stores K_{S_M} and MAC_S of a MAC address of the smart meter. The MDMS encrypts its MAC_M and T_M by the symmetric key K_{S_M} received from the smart meter and transmits it to the smart meter.

$$\begin{aligned} &\text{MDMS: } D(KS_M,\ E(KP_M, MAC_S \parallel\ K_{S_M} \parallel\ T_M)\ ) \\ &\text{MDMS: Stores } MAC_S,\ \ K_{S\_M} \\ &\text{MDMS} \rightarrow \text{Smart Meter: } E(K_{S\_M},\ \ MAC_M \parallel\ T_M) \end{aligned} \tag{14}$$

(3) The smart meter decrypts the message from the MDMS by the symmetric key K_{S_M}. , If the time stamp values are equal then the smart meter stores MAC_M in the smart meter and finishes the registration phase.

$$\begin{aligned} &\text{Smart Meter: } D(K_{S\_M},\ \ E(K_{S\_M},\ \ MAC_M \parallel T_M)) \\ &\text{Smart Meter: Stores } \ MAC_M \end{aligned} \tag{15}$$

3.2.6. Mutual Authentication phase between the Smart Meter and the MDMS and Transmission of Metering Information

Mutual Authentication phase between the Smart Meter and the MDMS and Transmission of Metering Information Registration phase between the Smart Meter and MDMS procedures are shown in Figure 7.

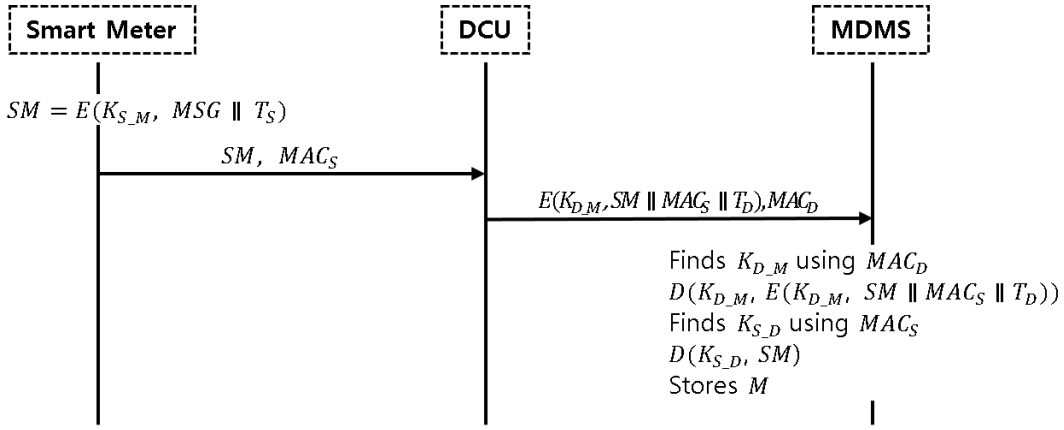

Figure 7. Mutual Authentication Phase Between the Smart Meter and the MDMS & Transmission of Metering Information

(1) The smart meter generates SM that has encrypted its metering information and its time stamp T_S by the symmetric key K_{S_M}. The smart meter transmits SM and MAC_S to the DCU.

$$\begin{aligned} &\text{SM: } SM = E(K_{S\_M}, MSG \parallel\ T_S\ ) \\ &\text{SM}\rightarrow\text{DCU: } SM, MAC_S \end{aligned} \tag{16}$$

(2) The DCU transmits its MAC address MAC_D and the message that has encrypts SM, MAC_S and T_D by the symmetric key K_{D_M} twice to the MDMS. In this phase, the DCU is impossible to check the SM of the metering information that has encrypted by the symmetric key K_{S_M} between the smart meter and the MDMS.

$$\text{DCU}\rightarrow\text{MDMS: } E(K_{D\_M}, SM \parallel MAC_S \parallel T_D), MAC_D \quad (17)$$

(3) The MDMS decrypts the message from the DCU by K_{D_M} gotten by using MAC_D. The MDMS decrypts SM from the smart meter by K_{S_M} gotten by using MAC_S and stores the secure metering information.

$$\begin{aligned}&\text{MDMS: Finds } K_{D\_M} \text{ using}\\&\text{MDMS: } D(K_{D\_M}, E(K_{D\_M}, SM \parallel MAC_S \parallel T_D)\\&\text{MDMS: Finds } K_{S\_M} \text{ using } MAC_S\\&\text{MDMS: } D(K_{S\_M}, SM)\\&\text{MDMS: Stores } M\end{aligned} \quad (18)$$

4. Analysis of the Proposed Protocol

The proposed scheme provides mutual authentication throughout the overall AMI environment to consider the DCU and the secure method to transmit group messages. The smart meter, the DCU and the MDMS generate the symmetric key to share the information in the registration phase. Each device is able to register each other again using the random value used when they are generating the symmetric key.

The smart meter guarantees security by transmitting the symmetric key and metering information for mutual authentication to the MDMS using the public key, the integrity by utilizing the hash operated key and the confidentiality using the secret value X that is encrypted. ID_*, P, Q, V and W values used in each authentication phase are protected from the replay attack by using the secret value X_* and the time stamp value generated every session in the MDMS.

This paper proposed a mutual authentication scheme between the smart meter and the DCU, the DCU and the MDMS, and the smart meter and the MDMS in the AMI environment. The DCU compares R_S with R_S', and the smart meter compares W and W' for mutual authentication between the smart meter and the DCU. The MDMS compares R_D with R_D' and the DCU compares Q and Q' for the mutual authentication between the DCU and the MDMS.

In the registration phase between the smart meter and the MDMS, the information encrypted twice and transmitted by the smart meter just passes through the DCU but is not stored in the DCU. The MDMS decrypts the double encrypted values by using K_{D_M} and K_{S_M}, and stores the metering information from the DCU since the MDMS received the K_{D_M} and K_{S_M} by MAC_D and MAC_S stored in the registration phase.

This protocol is intended to prevent the prediction of the encrypted metering information by attacking the DCU from the outside of the AMI environment, in the process that the smart meter transmits the metering information to the MDMS and it guarantees security by prohibiting the modulation of the metering information by encrypting the symmetric key generated between the smart meter and the MDMS, the DCU and the MDMS. This protocol has been designed to perform the mutual authentication between each device and to transmit the group message from many smart meters in the entire AMI environment.

5. Conclusion and the Future Work

The proposed authentication scheme in this paper is to ensure mutual authentication and secure transmission of the metering information in the entire AMI environment considering the DCU. The smart meter and the DCU, the DCU and the MDMS, the smart meter and the MDMS ensure information transmission and mutual authentication using the private key generated from each of the devices

and systems. The proposed scheme provides security against a replay attack using the time stamp in the registration and the authentication phases.

The metering information from the smart meter to the MDMS via the DCU is encrypted mutually using the private key generated between the smart meter and the MDMS, the DCU and the MDMS. The metering information transmitted from the smart meter to the DCU is impossible to be decrypted because of using the secret key between the smart meter and the MDMS, even though there would be many kinds of malicious attacks through the DCU.

This paper proposes the protocol of key exchanging and mutual authentication considering the DCU that has not been considered in other studies so far. The efficiency is decreased a bit because of increasing transmissions and the amount of data, because the proposed scheme adds the registration and authentication phases for increasing the stability that was not considered in the JY scheme.

However, efficiency decrement by increasing calculation amount is not a big issue, since accuracy and security are more important than speed when considering the characteristics of relationship of the smart meter and the DCU. The authentication between smart meter and the DCU becomes more important in the micro-grid environment to be realized shortly. The proposed scheme will be used as a base technique for the IoT communication to guarantee the security among each device in the Home Area Network of the AMI environment.

Acknowledgments

This work was supported by the Sun Moon University Research Grant of 2014.

References

[1] C. Lima, "Smart Grid Communications - Logical Reference Architecture", IEEE, **(2009)**.
[2] Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig and B. Sinopoli, "Cyber-Physical Security of a Smart Grid Infrastructure", Proceedings of the IEEE, **(2012)**.
[3] D. Kundur, X. Feng, S. Liu, T. Zourntos and K. Butler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid", Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm), **(2010)**; Gaithersburg, Maryland, USA.
[4] J. Choi and J. Seo, "Separate networks and an authentication framework in AMI for secure smart grid", Journal of the Korea Institute of Information Security and Cryptology, vol. 22, no. 3, **(2012)**, pp. 525–536.
[5] K. I. Jung, H. N. Park, B. G. Jung, J. S. Jang and M. A. Jung, "Smart Grid's Stability and Security Issues", the Korean Institute of Information Security and Cryptology, vol. 22, no. 5, **(2012)**, pp. 54-61.
[6] P. Siano, "Demand Response and smart grids: A survey", Renewable and Sustainable Energy Reviews, vol. 30, **(2014)**, pp. 461-478.
[7] F. M. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure(AMI)", Proceeding of Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st **(2008)**; Century, Pittsburgh, PA.
[8] S. H. Jeon, Y. A. Jung and S. S. Yeo, "Secure Metering Information Exchange Scheme Considering in AMI Environment", Proceedings of the Korea Navigation Institute Conference, **(2015)**; Seoul, Korea.
[9] H. G. Kim and I. Y. Lee, "A Study on ID-based authentication scheme in AMI SmartGrid environment", The KIPS transactions. Part C, vol. 18C, no. 6, **(2011)**, pp. 397-404.
[10] S. S. Yeo, D. I. Park and Y. A. Jung, "Enhanced ID-based Authentication Scheme using OTP in Smart Grid AMI Environment", Journal of Applied Mathematics, Hindawi, **(2014)**, pp.1-9.
[11] S. W. Hong, M. H. Lee and C. H. Lee, "Security risks and security requirement in the Korean Smart Grid", Communications of the Korean Institute of Information Scientists and Engineers, vol. 30, no. 1, **(2012)**, pp. 66-74.
[12] D. I. Park and S. S. Yeo, "ID-based Authentication Schemes with Forward Secrecy for Smart Grid AMI Environment", Journal of Korea Navigation Institute, vol. 17, no. 6, **(2013)**, pp. 736-748.

Author

Young-Ae Jung received her Ph.D. degree in Computer Science & Engineering from Dankook University, Korea. She is currently a professor at the Division of Information Technology Education, Sunmoon University, Korea. She has been serving as a Dean of IT Education Center, a Vice-Director of Glocal IT Fusion Training Center in Sunmoon University and a Vice-President of ICT Platform Society. Her research interests include Refactoring, Software Engineering, Security Engineering, Security, AI and Digital Humanities.