Privacy-Enhanced Secure Data Transaction System for Smart Grid

Woong Go and Jin Kwak*

ISAA Lab, Department of Information Security Engineering,
Soonchunhyang University, Korea
**Department of Information Security Engineering Soonchunhyang University, Korea*
wgo@sch.ac.kr, jkwak@sch.ac.kr

Abstract

A smart grid is a digitally enabled electrical grid that gathers, distributes, and acts on information about the behavior of all participants (suppliers and consumers) in order to improve the efficiency, importance, reliability, economics, and sustainability of electricity services. Currently, smart grid systems are widely considered to be fundamental components for improving the monitoring and control of a power distribution infrastructure. Using a distributed measurement architecture, it is possible to gather information about the smart grid status in order to monitor and control the overall infrastructure, including remote units. This technology can control the use of electricity. In particular, users can monitor and limit the electricity consumption of each home appliance in real time. Likewise, power companies can monitor and control electricity consumption in order to stabilize the electricity supply. However, these features may cause serious problems in the case of data leakage. For example, if a malicious attacker is able to sniff and analyze data, they can figure out the usage pattern and ascertain when a house is empty. Thus, users could suffer serious damage, such as burglary. Therefore, we propose a privacy-enhanced secure data transaction system. The proposed system can protect private data using encryption. The encrypted data includes the user's ID, home appliance serial number, and electricity consumption. Thus, attackers cannot obtain important data for analysis from transaction data. In addition, unauthorized power companies are unable to access this information.

Keywords: *Secure Data Transaction System, Smart Grid System, Privacy Protection, Electricity Consumption*

1. Introduction

Recently, environmental issues such as global warming have become more serious due to industrial emissions. Many studies into low-carbon green growth are being carried out around the world to solve these problems. The purpose of low-carbon green growth is the abatement of carbon dioxide emissions and efficient use of environmentally friendly resources. Thus, many researchers are studying application methods for these new technologies in various industries. Most of all, interest in smart grid as a method of making effective use of electricity is increasing.

A smart grid is a digitally enabled electrical grid that gathers, distributes, and acts on information about the behavior of all participants (suppliers and consumers) in order to improve the efficiency, importance, reliability, economics, and sustainability of electricity services [1, 2]. The interaction between users and power companies requires many sensitive items of information, such as user and home appliance information or smart meter information. This information should be transmitted securely. If it is not, a malicious attacker

could gather data on the electricity consumption of home appliances in order to determine the user's life pattern. This problem can lead to cases of burglary when no one is at home [3].

Therefore, we propose a data transaction protocol for privacy protection in a smart grid. This protocol has two phases: a transmission phase and a check phase. The purpose of the proposed scheme is to protect privacy and prevent further problems.

The remainder of this paper is organized as follows: In Section 2, we briefly provide fundamental knowledge about smart grid. In Section 3, we discuss security problems regarding private information in smart grid, and describe our proposed protocol in Section 4. We analyze the proposed protocol in Section 5, and, finally, summarize and conclude our research in Section 6.

2. Related work

2.1. Smart grid

A smart grid is a digitally enabled electrical grid that gathers, distributes, and acts on information about the behavior of all participants (suppliers and consumers) in order to improve the efficiency, importance, reliability, economics, and sustainability of electricity services. A smart grid communication network will comprise several different subsystems—it is truly a network of networks. These networks include supervisory control and data acquisition(SCADA), land mobile radio (LMR), cellular, microwave, fiber optic, dedicated or switched wirelines, RS-232/RS-485 serial links, wired and wireless Local Area Networks (LAN), or a versatile data network combining these media [1].

3. Security problems in smart grid systems

3.1. Data leakage

The security issues of smart grid have been widely discussed in recent years. Above all, the primary security issue is privacy, because information transmitted over a smart grid contains electricity usage patterns of home appliances. Moreover, this information could lead to disclosure of not only how much energy each user is consuming, but also when they are at home, at work, or traveling [4]. In addition, it might be possible to discover what types of home appliance are present by compromising users' home area networks.

Thus, if a criminal or malicious attacker can figure out when a user is not at home, they may break into the house at this time. Such energy-related information could support the criminal targeting of homes or provide business intelligence to competitors.

3.2. Illegal profiling

According to the Smart Metering & Privacy: Existing Law and Competing Policies report, researchers at MIT have developed a non-intrusive appliance load monitor (NALM) [5][6].

If NALMs could be appended to the existing metering infrastructure to allow for real-time logging of electricity consumption, information concerning appliance use may be reconstructed from the overall load data, thereby removing the need to intrude within the residential space and install new equipment within the home. NALMs were designed as research tools, set up to monitor only a small number of customers in order to facilitate load forecasting and management. However, smart grid allow for the collection and communication of highly detailed electricity usage information, in much the same way as the

NALM [6]. Thus, the problem of privacy within a smart grid is the most important security concern.

3.3. Illegal modification

Existing electricity companies require only power lines to connect the house to a power source. Thus, individual customers cannot access the electrical grid by the Internet. This feature provides security from the risks of the Internet. However, smart grid architecture not only connects to the electrical grid, but also the Internet. This means that smart grid are exposed to additional risks, one of which is illegal modification [7].

In a smart grid, users and electricity companies communicate with each other by wired or wireless network. Information about electricity consumption and user information will be transmitted via this network. Thus, if a malicious attacker modifies a user's electricity consumption, the user might pay a lot of money for electricity that has not been used. In addition, unscrupulous users could modify their electricity consumption in order to profit by paying less. Such cases have a high likelihood of occurrence.

4. Proposed protocol

4.1. Basic structure

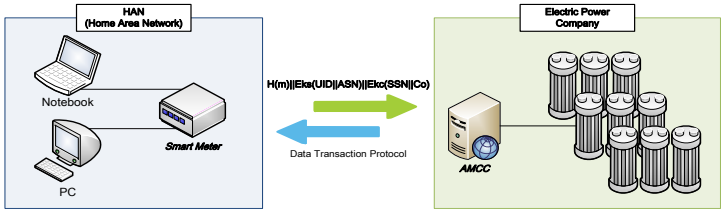

Figure 1. Overview of the proposed scheme

In this section, we propose a data transaction protocol for privacy protection. To solve the problems of existing smart grid systems, our scheme encrypts the information of home appliances. Thus, electricity companies or attackers cannot obtain any valuable information.

This scheme has two steps: a transmission phase and a check phase. In the transmission phase, the user sends encrypted information to the electricity company, such as electricity consumption and home appliances serial number(S/N), and the power company stores this information. In the check phase, the user requests their electricity consumption from the electricity company and can check the power consumption of each home appliance. Figure 2 shows an overview of the proposed scheme.

4.2. Entire scheme overview

Table 1 describes the notation for the proposed scheme. The following notation is used throughout this paper.

Table 1. Notation

Notation	Description	Notation	Description
U_{ID}	User ID (PIN, Citizen number, etc.)	Co	Electricity consumption
EPC	Electric power company	S_{SN}	Smart meter S/N
SM	Smart meter	r	Random nonce

A_{SN}	Home appliance S/N	$PRNG(\cdot)$	Pseudo-random number generator
$H(\cdot)$	Hash function		
Ks	User's password as an encryption/decryption key (between user and smart meter)		
Kc	Encryption/decryption key (between smart meter and electric power company)		

4.3. Transmission phase

In the transmission phase, information on home appliances and electricity consumption is transmitted securely. Thus, third parties do not know this information. In addition, the electric power company (*EPC*) only knows the electricity consumption. Thus, the users' private information, such as life pattern or kinds of home appliance, is protected.

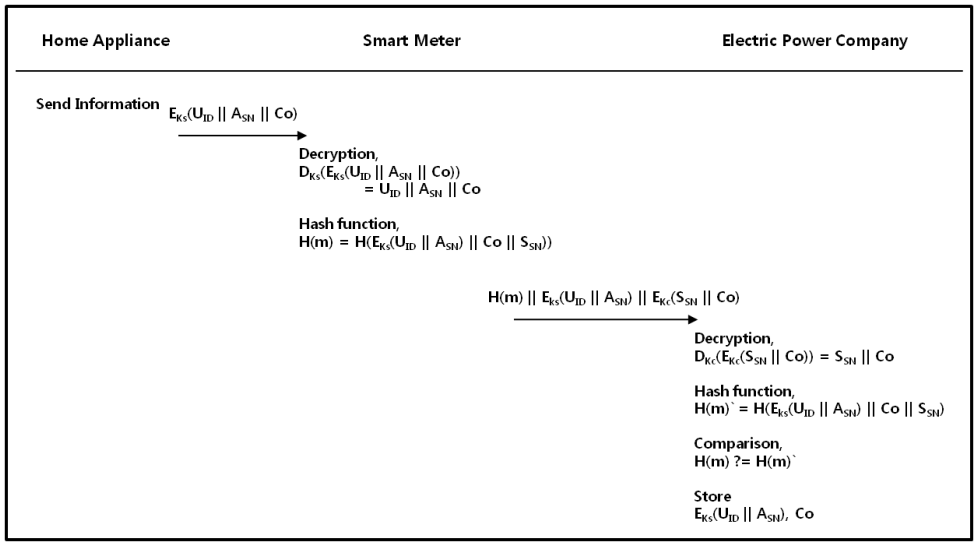

Figure 2. Transmission phase protocol

Each home appliance sends the user ID, home appliance serial number (A_{SN}), and electricity consumption (Co), encrypted by password (Ks), to the SM. And the SM decrypts the user ID, home appliance serial number, and electricity consumption, before encrypting the user ID and home appliance serial number using password Ks and creating hash data ($H(m)$) from the SM serial number and electricity consumption. This hash data will be used as an integrity check.

$$Home\ Appliance \rightarrow Smart\ Meter \qquad Smart\ Meter$$
$$E_{Ks}(U_{ID}\,||A_{SN}\,||Co) \qquad H(m) = H(E_{Ks}(U_{ID}\,||A_{SN}\,||Co||S_{SN})$$

Following this, the SM encrypts its serial number and the electricity consumption data using the encryption/decryption key (Kc), and sends this information to the EPC with the hash data and the encrypted user ID and home appliance serial number.

$$Smart\ Meter \rightarrow Electric\ Power\ Company$$
$$H(m)||E_{Ks}(U_{ID}\,||A_{SN})||E_{Kc}(S_{SN}\,||Co)$$

The EPC obtains the electricity consumption of the home appliance via the encrypted information ($E_{Kc}(S_{SN}\,||Co)$). Next, the EPC generates hash data ($H(m)'$) with the encrypted user ID and home appliance serial number, the SM serial number, and the electricity

consumption, and compares this with the received hash data ($H(m)$). If the comparison shows that the hash data is the same, the electricity consumption (Co) is stored with the encrypted information $E_{Ks}(U_{ID} || A_{SN})$.

Electric Power Company	*Comparison*	*Storage*
$H(m)' = H(E_{Ks}(U_{ID} \|\| A_{SN} \|\| Co \|\| S_{SN})$	$H(m)' \stackrel{?}{=} H(m)$	$E_{Ks}(U_{ID} \|\| A_{SN}), Co$

The encrypted information, $E_{Ks}(U_{ID} || A_{SN})$, will be used as an index of the home appliance. In addition, when a user requests the electricity consumption of any home appliance, the EPC can search for it using $E_{Ks}(U_{ID} || A_{SN})$ from the user.

4.4. Check phase

In this phase, a user requests the electricity consumption of one or many home appliances from the EPC.

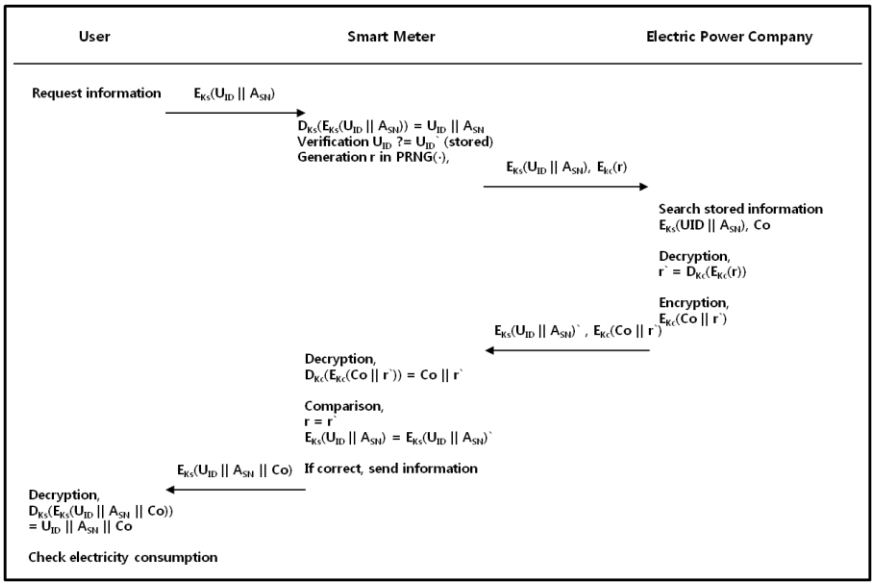

Figure 3. Check phase protocol

First, the user sends their encrypted user ID and home appliance serial number pertaining to the request about electricity consumption. And then, to verify that the request comes from an authorized user, the SM decrypts the user ID and home appliance serial number. The SM can verify the user ID from information stored in the previous step.

User $\rightarrow$ *Smart Meter*	*Smart Meter*
$E_{Ks}(U_{ID} \|\| A_{SN})$	$D_{Ks}(E_{Ks}(U_{ID} \|\| A_{SN}) = U_{ID} \|\| A_{SN} \Rightarrow U_{ID} \stackrel{?}{=} U_{ID}'$ $(stored)$

The SM then generates a random nonce (r) using the PRNG(·) function, and encrypts it with the encryption/decryption key. The purpose of the random nonce is the verification of electricity consumption from the EPC. Moreover, it can also prevent a man-in-the-middle (MITM) attack. Only an authorized EPC can receive and decrypt the random nonce, due to

the encryption/decryption key (Kc). Next, the SM sends the encrypted random nonce with the user ID and home appliance serial number.

$$\begin{array}{ll} Smart\ Meter & Smart\ Meter \rightarrow Electric\ Power\ Company \\ \quad Generation,\ r\ in\ PRNG(\cdot) & \quad E_{Ks}(U_{ID}\,||\,A_{SN}),\ E_{Kc}(r) \\ \quad E_{Kc}(r) & \end{array}$$

This encrypted information ($E_{Ks}(U_{ID}\,||\,A_{SN})$) allows the EPC to retrieve the electricity consumption of the home appliance from its database. In addition, the EPC decrypts the random nonce, and re-encrypts it along with the electricity consumption data.

$$\begin{array}{l} Electric\ Power\ Company \\ \quad Search\ electricity\ consumption\ by\ E_{Ks}(U_{ID}\,||\,A_{SN}) = Co \\ \quad Decryption\ and\ Encryption\ =>\quad D_{Kc}(E_{Kc}(r)) = r',\ E_{Kc}(CO\,||\,r') \end{array}$$

The EPC sends the stored encrypted user ID and home appliance serial number with the encrypted electricity consumption data and random nonce.

$$\begin{array}{l} Electric\ Power\ Company \rightarrow Smart\ Meter \\ \quad E_{Ks}(U_{ID}\,||\,A_{SN})',\ E_{Kc}(CO\,||\,r') \end{array}$$

The SM decrypts the random nonce and electricity consumption, and compares the initial random nonce (r) with the decrypted random nonce (r'). In addition, to verify that the correct electricity consumption data has been sent, the SM compares the user ID and home appliance serial number ($E_{Ks}(U_{ID}\,||\,A_{SN})$) between the stored and received information.

$$\begin{array}{ll} Smart\ Meter & Comparison \\ \quad Decryption & r \overset{?}{=} r' \\ \quad D_{Kc}(E_{Kc}(Co\,||\,r') = Co\,||\,r' & E_{Ks}(U_{ID}\,||\,A_{SN}) \overset{?}{=} E_{Ks}(U_{ID}\,||\,A_{SN})' \end{array}$$

If this comparison verifies that the sent data is correct, the SM sends the requested electricity consumption data to the user. Thus, the user can check the electricity consumption of their home appliances.

$$\begin{array}{ll} Smart\ Meter \rightarrow User & User \\ \quad E_{Ks}(U_{ID}\,||\,A_{SN}\,||Co) & \quad D_{Ks}(E_{Ks}(U_{ID}\,||\,A_{SN}\,||Co)) = U_{ID}\,||\,A_{SN}\,||Co \\ & \quad Check\ electricity\ consumption \end{array}$$

5. Analysis

5.1. Protection against data leakage

The proposed protocol protects against data leakage via a user password (Ks) and an encryption/decryption key (Kc). The user password is entered as a key between the home appliance and SM when the SM is first installed, and the encryption/decryption key is entered when the SM is produced. The target information from data leakage is the user ID and

electricity consumption. To discover when householders are at home, at work, or traveling, a malicious attacker would need this information.

However, the protocol proposed in this paper uses encrypted data. This contains the user ID, home appliance serial number, and electricity consumption ($E_{Ks}(U_{ID} || A_{SN} || Co)$). If a malicious attacker eavesdrops the encrypted information, they would need the user password (Ks) in order to decrypt it. Therefore, malicious attackers cannot decrypt this information so long as the user password is known only by the user.

5.2. Protection against illegal profiling

The proposed protocol protects against data leakage via a user password (Ks) and an encryption/decryption key (Kc). The user password is entered as a key between the home appliance and SM when the SM is first installed, and the encryption/decryption key is entered when the SM is produced. The target information from data leakage is the user ID and electricity consumption. To discover when householders are at home, at work, or traveling, a malicious attacker would need this information. In this paper, we encrypt the home appliance serial number (A_{SN}) by a user password (Ks) and encrypt electricity consumption data with a random nonce (r) using an encryption/decryption key (Kc) to protect against the above problem. Therefore, any intercepted home appliance or electricity consumption information is different from the real data.

5.3. Protection against illegal modification

If a malicious attacker modifies the electricity consumption data of some home appliance, the user may have to pay more money due to the modified information. On the other hand, if unscrupulous users modify their electricity consumption in order to profit, the EPC may suffer significant losses. Thus, the proposed protocol uses two keys (Ks, Kc) and a hash function ($H(\cdot)$) to protect against illegal modification. For example, if an attacker knows the encryption/decryption key (Kc) and attempts to modify the electricity consumption data in the transmission phase, the EPC can detect this illegal information.

- User = $\begin{matrix} H(m) = H(E_{Ks}(U_{ID} || A_{SN}) || Co || S_{SN})) \\ H(m) || E_{Ks}(U_{ID} || A_{SN}) || E_{Ks}(S_{SN} || Co) \end{matrix}$
- Attacker = $\begin{matrix} Computation, E_{Ks}(Co_A || S_{SNA}) \\ H(m) || E_{Ks}(U_{ID} || A_{SN}) || E_{Ks}(S_{SNA} || Co_A) \end{matrix}$
- EPC computes new hashed data and compares with received hashed data ($H(m)$).

  $Computation, H(m_A) = H(E_{Ks}(U_{ID} \| A_{SN}) \| Co_A \| S_{SNA}))$

  $Comparision, H(m) \stackrel{?}{=} H(m_A)$
- The comparison result shows that the received data is incorrect.
- Therefore, the EPC drops the attacker's transmission information.

6. Conclusion

In this paper, we proposed a secure data transaction protocol for smart grid to protect private information. The proposed protocol has two phases: a transmission phase and a check phase. In the transmission phase, we encrypted the user ID, home appliance serial number, and electricity consumption to protect against attacks such as eavesdropping, modification, and so on. For this, the proposed protocol used a user password, encryption/decryption key,

and hash function. In the check phase, the user could request information about the electricity consumption of a home appliance. For this, the user sent an encrypted user ID and home appliance serial number to the EPC. At that time, the SM generated a random nonce. The purpose of the random nonce was to protect electricity consumption data from illegal modification. Thus, the EPC sent the desired electricity consumption and random nonce in an encrypted state. The above features provide security to the data transaction, and thus the proposed scheme is expected to improve security.

References

[1] W. Wnag, Y. Xu, M. Khanna, "A Survey on the Communication Architectures in Smart Grid", Computer Networks, vol. 55, no. 15, **(2011)**.
[2] A. R. Metke and R. L. Ekl, "Smart Grid Security Technology", Proceedings of Innovative Smart Grid Technologies, **(2010)** January 19-21; Gothenburg, Sweden.
[3] W. Kehe, Z. Tong and L. Wei, "Research and Design of Security Defense Model in Power Grid Enterprise Information System", Proceedings of the International Conference on Multimedia Technology **(2010)** June 28-July 2; Malaga, Spain.
[4] H. Khurana, M. Hadley, N. Lu and D. A. Frincke, "Smart-grid Security Issues", IEEE Security and Privacy, vol. 8, no. 1, **(2010)**.
[5] S. Drenker, "Nonintrusive Monitoring of Electric Loads", IEEE Computer Applications in Power, vol. 12, no. 4, **(1999)**.
[6] E. L. Quinn, "Smart Metering and Privacy: Existing Laws and Competing Policies", Available at SSRN: http://ssrn.com/abstract=1462285 or http://dx.doi.org/10. 2139/ssrn.1462285, **(2009)**.
[7] S. D'Antonio, L. Coppolino, I.A. Elia and V. Formicola, "Security Issues of a Phasor Data Concentrator for Smart Grid Infrastructure", Proceedings of the 13th European Workshop on Dependable Computing, **(2011)** May 11-12; Pisa, Italy.

Authors

Woong Go

Woong Go received his BS and MS degree in Information Security from Soonchunhyang University, South Korea, in 2008 and 2010, respectively. And now he is working as a Ph.D candidate in the Information Security Application and Assurance Lab in the Soochunhyang University. His research interests include privacy protection, smart grid security and cloud computing security.

Jin Kwak

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. After that, he served MIC (Ministry of Information and Communication, Korea) as a Deputy Director. Also, he have served as a Dean of DISE(2009-2010) and Vice-Dean of College of Engineering (2009) in SCH. Now he is a Professor of Department of Information Security Engineering (DISE) at SCH. Also, now he is a Director of SCH BIT Business Incubation Center and a Director of Industry-University & Institute Partnership Division center at SCH. His main research areas are cryptology, information security applications and information assurance.