Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 829721, 9 pages
http://dx.doi.org/10.1155/2013/829721

Research Article

Privacy Protection Based Secure Data Transaction Protocol for Smart Sensor Meter in Smart Grid

Woong Go,[1] SeulKi Choi,[1] and Jin Kwak[2]

[1] *ISAA Lab, Department of Information Security Engineering, Soonchunhyang University, Asan, Chungchungnam-do 336-745, Republic of Korea*
[2] *Department of Information Security Engineering, Soonchunhyang University, Asan, Chungchungnam-do 336-745, Republic of Korea*

Correspondence should be addressed to Jin Kwak; jkwak@sch.ac.kr

Received 16 August 2013; Accepted 1 October 2013

Academic Editor: James J. Park

A smart grid is a data communications network integrated with an electrical grid that collects and analyzes near-real-time data on power transmission, distribution, and consumption. Currently, smart grid systems are considered to be necessary for improving the monitoring and control of a power distribution infrastructure. Using distributed measurement architecture, it is possible to gather information about the smart grid status for monitoring and controlling the overall infrastructure, including remote units. This architecture can control the use of electricity. In particular, users can monitor and regulate the electricity consumption of each home appliance in real time. Likewise, power companies can monitor and control electricity consumption for stabilizing electricity supply. However, serious problems can arise in case of data leakage. For example, if malicious attackers can sniff and analyze data, they can obtain the usage pattern of a house and ascertain when it is empty. They could then burgle the house. We propose a privacy-enhanced secure data transaction protocol that can protect private data by encrypting them. The encrypted data include the user's ID, home appliance serial number, and electricity consumption. Thus, attackers cannot obtain important data from the encrypted data. In addition, unauthorized power companies cannot access this information too.

1. Introduction

Recently, environmental issues such as global warming have become more serious because of industrial emissions. Many studies on low-carbon green growth are being carried out around the world to address them. The objective of aiming for low-carbon green growth is the abatement of carbon dioxide emissions and the efficient use of environmentally friendly resources. Thus, many researchers are studying application methods for these problems in various industries. In particular, interest in the use of smart grids for the effective use of electricity is increasing [1, 2].

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, reliability, economics, and sustainability of electricity services [3].

A key feature of smart grids is their ability to transmit information between the user and the electricity company in real time. In other words, users can check the electricity consumption of home appliances in real time, and electricity companies can generate only the electricity they need by analyzing usage patterns. The control of electricity production can help reduce carbon dioxide emissions. Interaction between users and power companies requires many types of sensitive information, such as user and home appliance information and smart sensor meter information. This information should be transmitted securely [4, 5]. Otherwise, a malicious attacker could gather data on the electricity consumption of home appliances in order to determine a user's routine and could plan a burglary when no one is at home.

We propose a privacy protection-based data transaction protocol for smart sensor meter in a smart grid. This protocol has two phases: a transmission phase and a check phase.

The remainder of this paper is organized as follows. In Section 2, we briefly provide basic information about smart grids. In Section 3, we discuss problems regarding

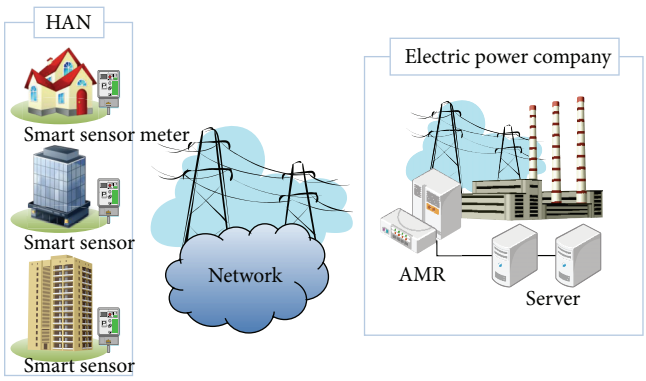

Figure 1: Smart grid system.

the security of private information in smart grids, while in Section 4, we describe our proposed protocol. We present an analysis of the proposed protocol in Section 5, and finally, we summarize 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, reliability, economics, and sustainability of electricity services (see Figure 1) [1].

A smart grid communication network will comprise several different subsystems—it is truly a network of networks. These networks include a supervisory control and data acquisition (SCADA) system; a land mobile radio (LMR) system; cellular, microwave, fiber optic, dedicated, or switched wirelines; RS-232/RS-485 serial links; wired and wireless local area networks (LAN), and so on [6, 7].

2.1.1. SCADA. An important component required for the monitoring and control of a substation is the SCADA system. It is utilized for distribution automation (DA) and computerized remote control of medium voltage (MV) substations and power grids, and it helps electricity utilities increase the reliability of power supply and reduce operating and maintenance costs. In the past, sectionalizer switchgear, ring main units, reclosers, and capacitor banks were designed for local operation with limited remote control capability. Today, using a SCADA system over reliable wireless communication links, remote terminal units (RTUs) provide powerful integrated solutions for upgrading remotely installed electrical equipment. In a Distribution Management System (DMS), RTUs seamlessly interface via a SCADA system with a wide range of high-performance control centers supplied by leading vendors worldwide. Connection to these Enterprise Management Systems (EMS) and DA/DMS control centers is typically provided via a high-performance IP Gateway or similar nodes [2, 8].

2.1.2. Wireless Networks. Different areas of the smart grid network require different wireless networking solutions. Advanced metering infrastructure (AMI) solutions can be meshed or point-to-point, with local coverage or long-range communication. Options for backhaul solutions are fiber, wireless broadband, or broadband over powerline, to name a few. Workforce mobility solutions include WiMax, WLAN, Cellular, and LMR, depending on the reliability, throughput, and coverage desired by the utility. Wireless communication solutions can be either licensed or unlicensed, again depending on the needs of the utility. For achieving the highest reliability, a licensed solution should be chosen. Each of the above options has advantages and disadvantages, but what is consistently true of all of them is the necessity of a scalable security solution [2, 9].

Table 1: Notation of Ren et al.'s scheme.

Notation	Description
UN	User name
SM	Smart meter
SGCC	Smart grid control center
TTP_{PubK}	Public key of TTP
V	Value of automatic meter readings
MK	Preloaded master key
SIK	Session integrity key
AID	Anonymous ID
TTP	Trusted third party
USR	User
TTP_{PriK}	Private key of TTP
LocID	Location ID
SEK	Session encryption key
$\|$	Concatenation

2.1.3. Security. Smart grid deployments must meet stringent security requirements. Strong authentication is necessary for all users and devices that may affect the operation of the grid. With the large number of users and devices affected, scalable key and trust management systems, customized to the specific needs of the energy service provider, are essential.

The deployment and operation of large, secure network communication systems over many years has taught us that the effort required to provision symmetric keys into thousands of devices can be too expensive or insecure. The development of key and trust management systems for large network deployments is required; these systems can be adopted from other industries, for example, LMR systems and Association of Public-Safety Communications Officials (APCO) radio systems. Several APCO-deployed systems provide statewide wireless coverage, with tens of thousands of secure devices. Trust management systems based on public key infrastructure (PKI) technology could be specifically customized for smart grid operators, easing the burden of providing security that adheres to accepted and guidelines that are known to be secure [10, 11].

2.2. Review of Ren et al.'s Scheme. In this section, we present an analysis of Ren et al.'s scheme [12] (see Table 1). These

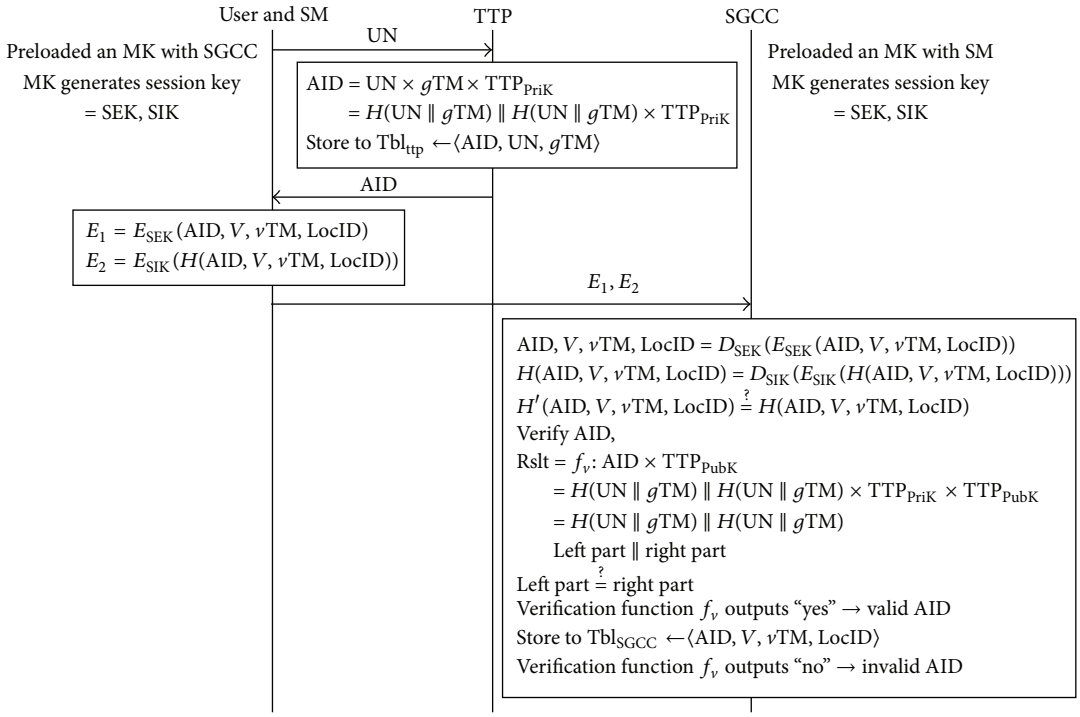

Figure 2: Protocol of Ren et al.'s scheme.

researchers proposed lightweight privacy-aware yet accountable secure communication scheme (PASS) between SM sensors and a Smart Grid Control Center (SGCC). PASS has five components: AID generation, attaching AID, uploading data, AID verification, and AID traceability.

(1) AID generation: the customer presents a UN to a TTP. The TTP generates the corresponding AID by using the generation function:

$$\left(f_g : \mathrm{UN} \times g\mathrm{TM} \times \mathrm{TTP}_{\mathrm{PriK}} \longrightarrow \mathrm{AID}\right), \quad (1)$$

where gTM is the time-stamp used for the AID generation. After the AID generation, the TTP returns the AID to the customer and stores an item in a table called $\mathrm{Tbl}_{\mathrm{ttp}}$, which stores tuples $\langle \mathrm{AID}, \mathrm{UN}, \text{ and } g\mathrm{TM}\rangle$.

(2) Attaching AID: the customer inputs the obtained AID into a SM at his/her residence.

(3) Data uploading: the customer uploads data messages E_1 and E_2 (defined below). The SGCC creates a table called $\mathrm{Tbl}_{\mathrm{sgcc}}$, in which tuples $\langle \mathrm{AID}, V, v\mathrm{TM}, \text{and LocID}\rangle$ are stored. vTM is the time-stamp for uploading the data.

Consider

$$E_1 = E_{\mathrm{SEK}}(\mathrm{AID}, V, v\mathrm{TM}, \mathrm{LocID}),$$
$$E_2 = E_{\mathrm{SIK}}(H(\mathrm{AID}, V, v\mathrm{TM}, \mathrm{LocID})). \quad (2)$$

(4) AID verification: the SGCC decrypts the uploaded data and examines whether the AID is valid and whether it has been forged by a malicious user. The verification function is $f_g : \mathrm{AID} \times \mathrm{TTP}_{\mathrm{PubK}} \rightarrow \mathrm{Rslt}$. If Rslt has a "given" *a priori* pattern; that is, its left half and right half are identical, the verification function outputs "Yes," which means the AID is valid. Otherwise, the output is "No," which means the AID is invalid.

(5) AID traceability: the SGCC can trace back to AID's LocID. However, it cannot recover the UN of the AID by itself. Only the TTP can recover the AID. Given the AID, TTP fetches $\langle \mathrm{UN}, g\mathrm{TM}\rangle$ from $\mathrm{Tbl}_{\mathrm{ttp}} = \langle \mathrm{AID}, \mathrm{UN}, g\mathrm{TM}\rangle$ and checks whether the following equation is satisfied:

$$\mathrm{AID} \times \mathrm{TTP}_{\mathrm{PubK}} = H\left(\mathrm{UN} \parallel g\mathrm{TM}\right) \parallel H\left(\mathrm{UN} \parallel g\mathrm{TM}\right). \quad (3)$$

If it is satisfied, the TTP can confirm that the "opened" TTP is the UN, and such a UN is not repudiated.

3. Security Problems in Smart Grid Systems

3.1. Privacy Problem. The security issues in smart grid have been widely discussed in recent years. The primary security issue is privacy because information transmitted over a smart grid contains electricity usage patterns of home appliances. This information could indicate not only the amount of energy consumed by each user, but also when they are at home, at work, or traveling [13]. Furthermore, it might be

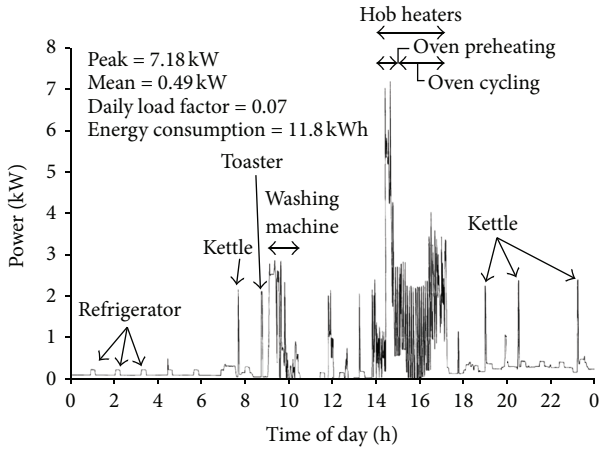

Figure 3: Household electricity demand profile recorded on a one minute time base.

possible to infer what types of home appliances are present by compromising users' home area networks. The present smart grid system gathers user information in order to check and calculate the amount of electricity consumption.

Thus, if a criminal or malicious attacker can determine when a user is not at home, they may break into his/her house at such a time. Thus, energy-related information could support burglars or provide business intelligence to competitors [14].

3.2. Electricity Consumption Loss. According to the report Smart Metering & Privacy: Existing Law and Competing Policies, researchers at MIT have developed a nonintrusive appliance load monitor (NALM) [15, 16].

If NALMs could be incorporated in 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 residential space and install new equipment in the house. NALMs were designed as research tools, and they were set up to monitor only a small number of customers in order to facilitate load forecasting and management (see Figure 3). However, smart grids allow the collection and communication of highly detailed electricity usage information, in much the same way as the NALM [16]. Thus, the problem of privacy within a smart grid is the main concern.

3.3. Modification of Electricity Consumption. Existing power companies require only power lines to connect a house to a power source. Thus, individual customers cannot access the electrical grid through the Internet. This feature provides security from the risks associated with the Internet. However, smart grid architecture connects a house (smart sensor network) to not only an electrical grid but also the Internet. This means that a smart grid is exposed to additional risks, one of which is illegal modification of electricity consumption [17].

Table 2: Notation used for the proposed.

Notation	Description
PC	Power company
HA	Home appliance
SN_{HA}	Home appliance serial number
SN_{list}	List of smart sensor meter serial number
Kus	User's password as an encryption/decryption key (between user and smart sensor meter)
r	Random nonce
$H(\cdot)$	Hash function
E_n	Encrypted data
SM	Smart sensor meter
ID_U	User ID
SN_{SM}	Smart sensor meter serial number
EC	Electricity consumption
Ksp	Encryption/decryption key (between smart sensor meter and power company)
PRNG(·)	Pseudorandom number generator
H_n	Hashed data

In a smart grid, users and electricity companies communicate with each other through a wired or wireless network. Information about electricity consumption and the user is transmitted via this network. Thus, if a malicious attacker modifies a user's electricity consumption, the user might have to pay a lot of money for electricity that has not actually been used. In addition, unscrupulous users could modify their electricity consumption in order to profit by paying less. There is a high likelihood of such instances [18].

4. Proposed Protocol

4.1. Basic Structure. In this section, we propose a data transaction protocol for privacy protection (see Figure 2). To solve the problems faced in existing smart grid systems, our scheme creates hash data from the information on 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 former, the user sends encrypted information, such as electricity consumption and serial numbers of home appliances, to the power company and the power company stores this information. In the check phase, the user requests his/her electricity consumption from the power company and can check the power consumption of each home appliance. Figure 4 shows an overview of the proposed scheme.

4.2. Overview of Entire Scheme. Table 2 describes the notation used for discussing the proposed scheme. The notation is used throughout this paper.

4.3. Registration Phase. In the registration phase, the user inputs his/her ID (ID_U) and password (Kus) by using a smart

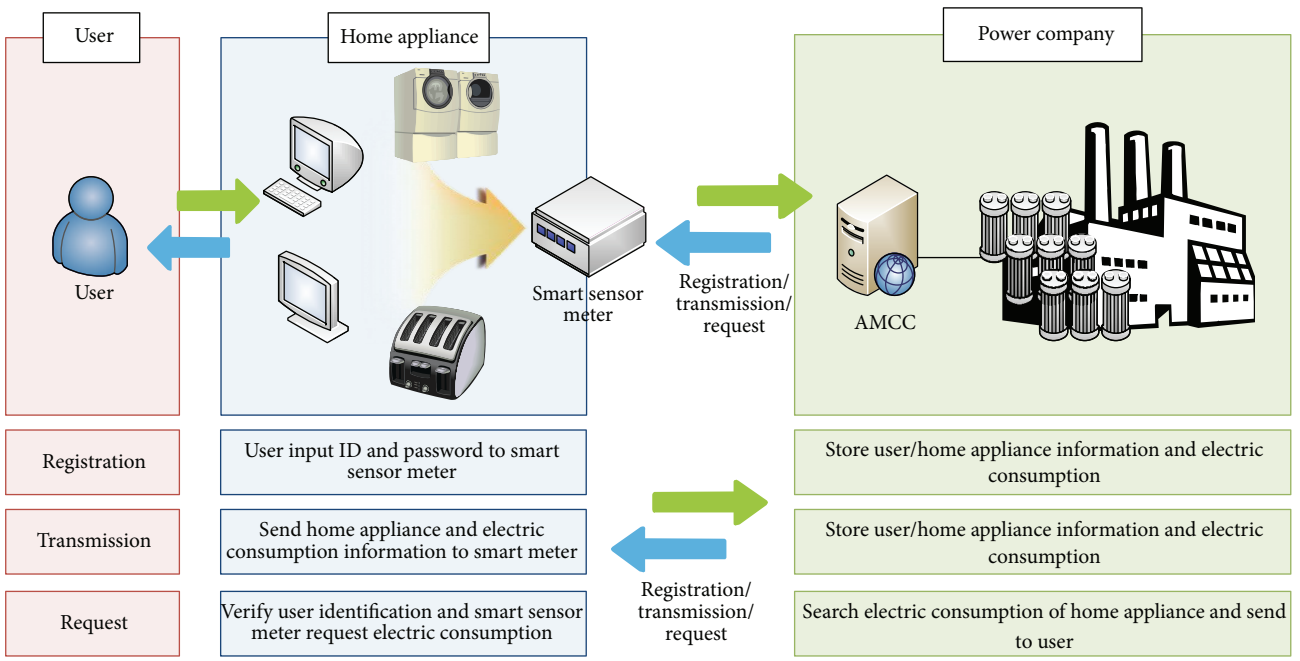

Figure 4: Overview of the proposed scheme.

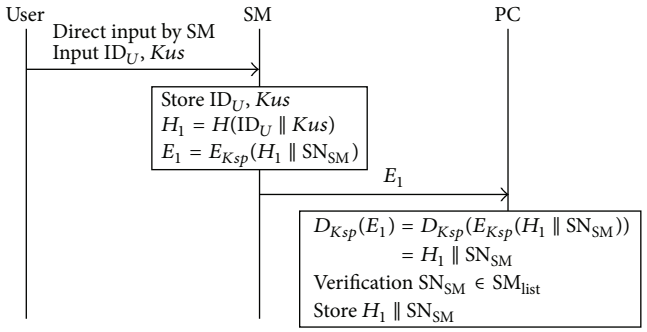

Figure 5: Registration phase.

sensor meter (SM) display. The SM display is the interface between the user and the SM (see Figure 5).

The SM sends these information to the power company (PC), and the PC stores the information. The information is used as the user's identity and encryption/decryption key between the user and SM. Moreover, the PC does not have knowledge of these information because the ID_U and Kus are hashed before communication.

When the user moves into a new house, he/she should register his/her ID_U and Kus with the SM

$$\begin{aligned} &\text{User} \longrightarrow \text{Smart Meter} \\ &\text{Input } ID_U, Kus. \end{aligned} \tag{4}$$

The SM stores the ID_U and Kus and creates hash data (H_1) from these information. This hash data are used as the user identification and for extracting electricity consumption (EC) from other data ($H_1 \oplus$ EC). Then, the hash data (H_1) and SM serial number (SN_{SM}) are encrypted (E_1) with an encryption/decryption key (Ksp). The SM sends the encrypted data the PC

$$\begin{aligned} &\text{Smart Meter} \\ &\quad \text{Store } ID_U, Kus, \\ &\quad H_1 = H(ID_U \| Kus), \\ &\quad E_1 = E_{Ksp}(H_1 \| SN_{SM}), \\ &\text{Smart Meter} \longrightarrow \text{Power Company} \\ &\quad E_1 = E_{Ksp}(H_1 \| SN_{SM}). \end{aligned} \tag{5}$$

The PC decrypts the hash data (H_1) and SM serial number (SN_{SM}) obtained from E_1. Then, the SM verifies the SM serial number (SN_{SM}) by checking if it exists in the list of SMs (SN_{list}). If the SM serial number is valid, the PC stores these information ($H_1 \| SN_{SM}$)

$$\begin{aligned} &\text{Power Company} \\ &\quad D_{Ksp}(E_1) = D_{Ksp}(E_{Ksp}(H_1 \| SN_{SM})) \\ &\qquad = H_1 \| SN_{SM}, \\ &\quad \text{Verification } SN_{SM} \in SM_{list}, \\ &\quad \text{Store } H_1 \| SN_{SM}. \end{aligned} \tag{6}$$

4.4. Transmission Phase. In the transmission phase, information on home appliances (HA) and electricity consumption (EC) is transmitted securely (see Figure 6). Thus, third parties and the PC do not have any knowledge of this information. In addition, the PC only knows the electricity consumption.

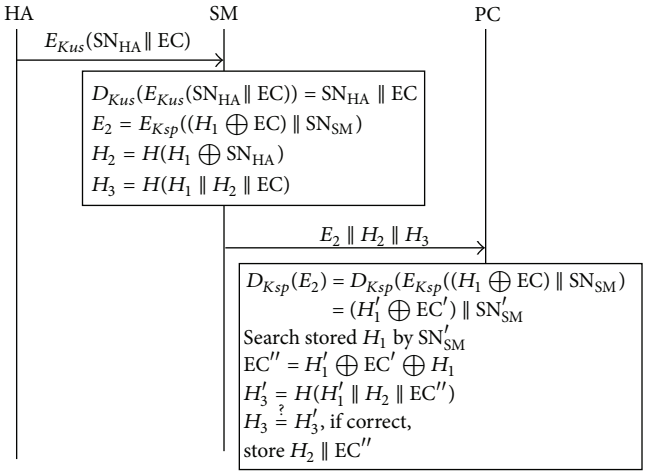

Figure 6: Transmission phase.

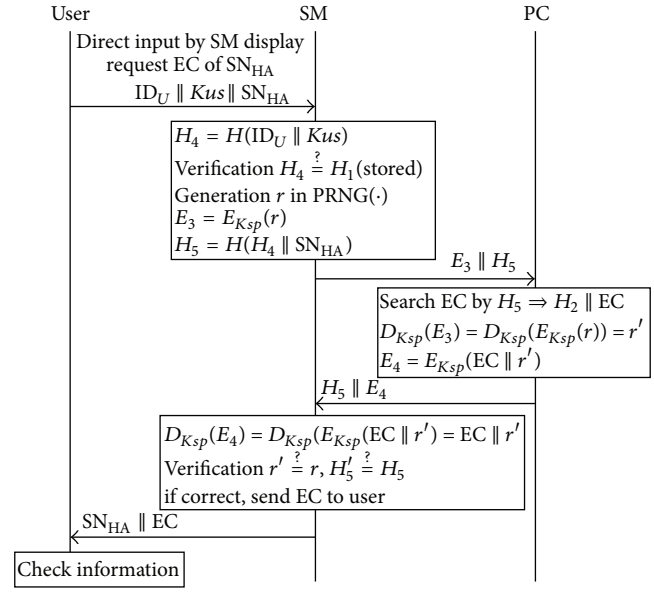

Figure 7: Check phase.

Thus, the user's private information, such as daily routine or the home appliances possessed by him/her, is protected.

Each home appliance sends the home appliance serial number ($\mathrm{SN_{HA}}$) and electricity consumption (EC), encrypted with Kus, to the SM

$$\begin{aligned} &\text{Home Appliance} \longrightarrow \text{Smart Meter} \\ &E_{Kus}\left(\mathrm{SN_{HA}} \parallel \mathrm{EC}\right). \end{aligned} \tag{7}$$

The SM decrypts the home appliance serial number ($\mathrm{SN_{HA}}$) and electricity consumption (EC) before encrypting the hash data (H_1), electricity consumption (EC), and SM serial number ($\mathrm{SN_{SM}}$) with Ksp and creating hash data (H_2) from H_1 and the HA serial number ($\mathrm{SN_{HA}}$). Then, the two sets of hash data (H_1, H_2) and electricity consumption (EC) are hashed (H_3). H_3 is used for performing an integrity check. The SM then sends encrypted data (E_2) with the two sets of hash data (H_2, H_3) to the PC

$$\begin{aligned} &\text{Smart Meter} \\ &D_{Kus}\left(E_{Kus}\left(\mathrm{SN_{HA}} \parallel \mathrm{EC}\right)\right) = \mathrm{SN_{HA}} \parallel \mathrm{EC}, \\ &E_2 = E_{Ksp}\left(\left(H_1 \oplus \mathrm{EC}\right) \parallel \mathrm{SN_{SM}}\right), \\ &H_2 = H\left(H_1 \oplus \mathrm{SN_{HA}}\right), \\ &H_3 = H\left(H_1 \parallel H_2 \parallel \mathrm{EC}\right), \\ &\text{Smart Meter} \longrightarrow \text{Power Company} \\ &E_2 \parallel H_2 \parallel H_3. \end{aligned} \tag{8}$$

The PC obtains $H_1' \oplus \mathrm{EC}'$ and the SM serial number ($\mathrm{SN_{SM}}'$) via the encrypted information (E_2). Next, the PC searches the stored H_1 by using $\mathrm{SN_{SM}}'$ and extracts the electricity consumption (EC'') from $H_1' \oplus \mathrm{EC}'$ by using the stored H_1. After the extraction is complete, the PC creates hash data (H_3') from H_1', H_2, and EC'' and makes a comparison between the received H_3 and H_3'. If the comparison shows that the hash data are identical, the EC is stored with the hashed information H_2

$$\begin{aligned} &\text{Power Company} \\ &D_{Ksp}\left(E_2\right) = D_{Ksp}\left(E_{Ksp}\left(\left(H_1 \oplus \mathrm{EC}\right) \parallel \mathrm{SN_{SM}}\right)\right) \\ &\qquad = \left(H_1' \oplus \mathrm{EC}'\right) \parallel \mathrm{SN_{SM}}', \\ &\text{Search sorted } H_1 \text{ using } \mathrm{SN_{SM}}' \\ &\mathrm{EC}'' = H_1' \oplus \mathrm{EC}' \oplus H_1, \\ &\text{Comparison } H_3 \stackrel{?}{=} H_3', \\ &\text{If correct, store } H_2 \parallel \mathrm{EC}''. \end{aligned} \tag{9}$$

H_2 is used as an index of the home appliance. In addition, when a user requests the electricity consumption of any home appliance, the PC can search for it using H_2 obtained from the user.

4.5. Check Phase. In this phase, the user requests the electricity consumption of one or more home appliances from the PC (see Figure 7).

First, the user inputs the ID_U and Kus along with the serial number ($\mathrm{SN_{HA}}$) of the home appliance whose electricity consumption is required

$$\begin{aligned} &\text{User} \longrightarrow \text{Smart Meter} \\ &U_{\mathrm{ID}} \parallel Kus \parallel \mathrm{SN_{HA}}. \end{aligned} \tag{10}$$

To verify that the request has come from an authorized user, the SM creates hash data (H_4) by using the data input by the user ($U_{\mathrm{ID}} \parallel Kus$). It then verifies the user from the information stored in the registration phase. After user verification, the SM generates random nonce (r) by using the PRNG(·) function and encrypts it with Ksp. The purpose of generating r is for facilitating the verification of the electricity consumption by the user when he/she receives information from the PC. Hash data (H_5) are generated in order to search stored electricity consumption values. Lastly, the SM sends encryption data and hash data ($E_3 \parallel H_5$) to the PC

$$\begin{aligned}
&\text{Smart Meter}\\
&H_4 = H\left(\mathrm{ID}_U \parallel Kus\right),\\
&\text{Verification } H_4 \stackrel{?}{=} H_1 \text{ (stored)},\\
&\text{Generation of } r \text{ in PRNG}(\cdot),\\
&E_3 = E_{Ksp}(r),\\
&H_5 = H\left(H_4 \parallel \mathrm{SH}_{\mathrm{HA}}\right),\\
&\text{Smart Meter} \longrightarrow \text{Power Company}\\
&E_3 \parallel H_5.
\end{aligned} \tag{11}$$

H_5 allows the PC to retrieve the EC of the home appliance from its database. Further, random nonce (r') is decrypted from the received information (E_3). Subsequently, the PC encrypts the EC and r' with Ksp. All computed data ($H_5 \parallel E_4$) are sent to the SM

$$\begin{aligned}
&\text{Power Company}\\
&\text{Search EC by } H_5 \Longrightarrow H_2 \parallel \mathrm{EC},\\
&D_{Ksp}\left(E_3\right) = D_{Ksp}\left(E_{Ksp}(r)\right) = r',\\
&E_4 = E_{Ksp}\left(\mathrm{EC} \parallel r'\right),\\
&\text{Power Company} \longrightarrow \text{Smart Meter}\\
&H_5 \parallel E_4.
\end{aligned} \tag{12}$$

When $H_5 \parallel E_4$ are received, the SM decrypts the EC and r' and makes a comparison between the initial random nonce r and the decrypted random nonce (r'). If the random nonce comparison result is not correct, it means that E_4 has been modified. Thus, the SM discards the data. Similarly, H_5' should be compared with the initial hash data H_5. If these two comparisons indicate that the sent data are correct, the SM sends the requested electricity consumption (EC) with the home appliance serial number ($\mathrm{SN}_{\mathrm{HA}}$) to the user

$$\begin{aligned}
&\text{Smart Meter}\\
&D_{Ksp}\left(E_4\right) = D_{Ksp}\left(E_{Ksp}\left(\mathrm{EC} \parallel r'\right)\right) = \mathrm{EC} \parallel r',\\
&\text{Verification } r \stackrel{?}{=} r',\ H_5 \stackrel{?}{=} H_5',\\
&\text{If correct, send EC to User.}
\end{aligned} \tag{13}$$

Finally, the user can check the electricity consumption of his/her home appliances.

5. Analysis

5.1. Protection against Privacy Invasion. The proposed protocol protects against privacy invasion by using a user password (Kus) and an encryption/decryption key (Ksp). 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 manufactured. The target information necessary for privacy invasion is the user ID, home appliance serial number, and electricity consumption. To determine when the user is 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 home appliance serial number and electricity consumption ($E_{Kus}(\mathrm{SN}_{\mathrm{HA}} \parallel \mathrm{EC})$). If a malicious attacker eavesdrops on the encrypted information, they would need the user password (Kus) to decrypt it. Therefore, malicious attackers cannot decrypt this information as long as the user password is known only to the user.

5.2. Protection against Electricity Consumption Loss. The proposed protocol protects against data leakage by using a user password (Kus), an encryption/decryption key (Ksp), and random nonce (r). The target information is the home appliance serial number ($\mathrm{SN}_{\mathrm{HA}}$) and electricity consumption (EC). To determine when the user is at home, at work, or traveling, a malicious attacker would need this information.

In the transmission phase, we encrypt the home appliance serial number ($\mathrm{SN}_{\mathrm{HA}}$) and electricity consumption (EC) by using the user password (Kus). In addition, this electricity consumption and hash data (H_1) are computed using the exclusive-OR operation. Additionally, the PC encrypts the electricity consumption with a random nonce (r) using an encryption/decryption key (Ksp) in the check phase. The use of the exclusive-OR operation and random nonce makes it difficult to extract the electricity consumption. Therefore, any intercepted home appliance electricity consumption information is different from the real data.

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

Table 3: Analysis of computational cost.

	Computation	Proposed scheme	Ren et al. [12]
Registration	Asymmetric encryption	—	—
	Symmetric encryption	2Sym	—
	Hash function	1T (h)	—
Transmission (PASS)	Asymmetric encryption	—	2Asym
	Symmetric encryption	4Sym	4Sym
	Hash function	3T (h)	4T (h)
Request	Asymmetric encryption	—	—
	Symmetric encryption	3Sym	—
	Hash function	3T (h)	—

Consider

(i)

$$E_2 = E_{Ksp}\left((H_1 \oplus \mathrm{EC}) \parallel \mathrm{SN_{SM}}\right),$$
$$\mathrm{SM} \Longrightarrow H_2 = H\left(H_1 \oplus \mathrm{SN_{HA}}\right), \quad H_3 = H\left(H_1 \parallel H_2 \parallel \mathrm{EC}\right),$$
$$\text{Send } E_2 \parallel H_2 \parallel H_3 \text{ to PC.} \tag{14}$$

(ii)

Attacker

$$\Longrightarrow \text{Computation, } E_{2A} = E_{Ksp}\left((H_{1A} \oplus \mathrm{EC}_A) \parallel \mathrm{SN_{SMA}}\right)$$
$$\text{Send } E_{2A} \parallel H_2 \parallel H_3 \text{ to PC.} \tag{15}$$

(iii) Attacker cannot create H_2 and H_3 because he/she does not know H_1.

(iv) The PC extracts electricity consumption using exclusive-OR operation.

(v) The PC computes new hashed data (H_3') and compares them with received hashed data (H_3)

$$\mathrm{EC}_A = \left(H_{1A} \oplus \mathrm{EC}_A\right) \oplus H_1,$$
$$H_{3A} = H\left(H_1 \parallel H_2 \parallel \mathrm{EC}_A\right), \qquad H_3 \stackrel{?}{=} H_{3A} \text{ (incorrect)}. \tag{16}$$

(vi) The comparison result shows that the received data is incorrect.

(vii) Therefore, the PC discards the information transmitted by the attacker.

5.4. Performance Analysis. In this section, we compare the performance of our proposed scheme with that of Ren et al.'s scheme. The proposed scheme has three phases: registration, transmission, and request. In contrast, Ren et al.'s scheme has only one phase, called PASS. PASS is similar to the transmission phase of the proposed scheme. Therefore, we compare PASS and the transmission phase.

Table 4: Analysis of communication cost.

	Proposed scheme	Ren et al. [12]
Registration	2	—
Transmission (PASS)	2	3
Request	4	—

Table 3 shows an analysis of the computational cost. The proposed scheme is computationally more efficient compared to Ren et al.'s scheme. Besides, in the former, asymmetric encryption is not used and the hash function is used less.

Table 4 shows an analysis of the communication cost. As can be seen, our proposed scheme needs two handshakes in the transmission phase. On the other hand, Ren et al.'s scheme needs three handshakes in PASS. Thus, our proposed scheme is more efficient with regard to the communication cost.

In order to compare the proposed scheme and Ren et al.'s scheme, we simplify the computational cost for carrying out a quantitative analysis. We assume that the computational cost of asymmetric encryption, symmetric encryption, and the hash function are 3, 2, and 1, respectively. Actually, asymmetric encryption involves higher computational cost compared to symmetric encryption and the hash function. Further, symmetric encryption involves higher computational cost compared to the hash function. Thus, the computational cost of the proposed scheme is 11 (4Sym + 3T (h) = 4 × 2 + 3 × 1 = 11), while that of Ren et al.'s scheme is 18 (2Asym + 4Sym + 4T (h) = 2 × 3 + 4 × 2 + 4 × 1 = 18).

Figure 8 shows the changes in the computational cost and communication cost with time. We calculate the costs for the case where data are transmitted at regular intervals. For example, if data are transmitted at 10 min intervals (144 = 1 day/10 min), the cost of the proposed scheme is 1584 (= 144 × 11), while that of Ren et al.'s scheme is 2592 (= 144 × 18).

6. Conclusion

In this paper, we have proposed a secure data transaction protocol for smart grids to protect private information. The proposed protocol has two phases: a transmission phase and a check phase. In the former, we encrypt the user ID, home appliance serial number, and electricity consumption to protect against attacks such as eavesdropping and modification. For the encryption, the user password, encryption/decryption key, and hash function are used. In the check phase, the user can request information about the electricity consumption of a home appliance. For this, he/she sends an encrypted user ID and home appliance serial number to the PC. And the SM generates a random nonce. The purpose of generating the random nonce is to protect electricity consumption data from illegal modification. Thus, the PC sends the desired electricity consumption and random nonce in an encrypted state. The above features provide security to the data transaction.

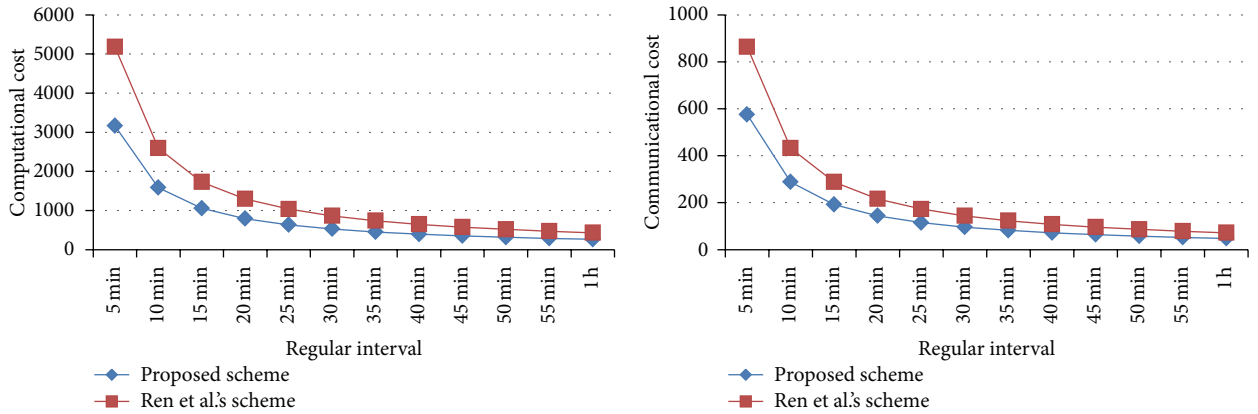

Figure 8: Changes in computational and communication cost for data transmission at regular intervals.

Conflict of Interests

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This research was supported by the Ministry of Knowledge Economy (MKE), Republic of Korea, under the Information Technology Research Center (ITRC) support program (NIPA-2012-H0301-12-3007) supervised by the National IT Industry Promotion Agency (NIPA). This work was supported by the Soonchunhyang University Research Fund.

References

[1] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, no. 15, pp. 3604–3629, 2011.

[2] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Proceedings of the Innovative Smart Grid Technologies*, January 2010.

[3] S. Adwitiya and K. L. Daya, "Performance evaluation of data aggregation for cluster-based wireless sensor network," *Human-Centric Computing and Information Sciences*, vol. 3, pp. 1–17, 2013.

[4] Y. Min, K. Yong-Ki, and C. Jae-Woo, "An energy-efficient routing protocol using message success rate in wireless sensor networks," *Journal of Covenvergence*, vol. 4, pp. 15–22, 2013.

[5] R. Sumathi and M. G. Srinivas, "A survey of QoS based routing protocols for wireless sensor networks," *Journal of Information Processing Systems*, no. 8, pp. 589–602, 2012.

[6] R. S. Tolentino and T.H. Kim, "Review: distributed system network architecture for securing SCADA system," *International Journal of Smart Home*, vol. 4, no. 1, pp. 13–22, 2010.

[7] U. Ahmad and H. S. Sajjad, "Evolution of communication technologies for smart grid applications," *Revewable and Sustainable Energy Revies*, vol. 19, pp. 191–199, 2013.

[8] K. Dong-Joo and P. Sunju, "A conceptual approach to data visualization for user interface design of smart grid operation tools," *International Journal of Energy, Information and Communications*, no. 1, pp. 64–76, 2010.

[9] A. Emilio, B. Raffaele, and C. Marco, "The role of communication systems in smart grids: architectures, technical solutions and research challenges," *Computer Communications*, 2013.

[10] K. Wu, T. Zhang, and W. Li, "Research and design of security defense model in power grid enterprise information system," in *Proceedings of the International Conference on Multimedia Technology (ICMT '10)*, October 2010.

[11] J. R. Rosslin and C. Min-kyu, "Assessment of the vulnerabilities of SCADA, control systems and critical infrastructure systems," *International Journal of Grid and Distributed Computing*, vol. 2, pp. 27–34, 2009.

[12] W. Ren, J. Song, Y. Yang, and Y. Ren, "Lightweight privacy-aware yet accountable secure scheme for SM-SGCC communications in smart grid," *Tsinghua Science and Technology*, vol. 16, no. 6, pp. 640–647, 2011.

[13] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[14] R. Cristina, V. Giacomo, and C. Antonio, "Privacy-preserving smart metering with multiple data consumers," *Computer Netowkrs*, vol. 57, pp. 1699–1713, 2013.

[15] S. Drenker and A. Kader, "Nonintrusive monitoring of electric loads," *IEEE Computer Applications in Power*, vol. 12, no. 4, pp. 47–51, 1999.

[16] E. L. Quinn, "Smart metering and privacy: existing laws and competing policies," Tech. Rep., 2009, http://ssrn.com/abstract=1462285, http://dx.doi.org/ 10.2139/ssrn.1462285.

[17] S. D'Antonio,, L. Coppolino, I. A. Elia, and V. Fromicola, "Security issues of a phasor data concentrator for smart grid infrastructure," in *Proceedings of the 13th European Workshop on Dependable Computing (EWDC '11)*, pp. 3–8, May 2011.

[18] W. Wenye and L. Zhuo, "Cyber security in the smart grid: survey and challenges," *Computer Networks*, no. 57, pp. 1344–1371, 2013.