석사 학위논문

Master's Thesis

스마트 그리드 시스템의 댁내망에서 개인정보 보호를 위한 인증 기법 연구

A Study on Privacy-preserving Authentication Scheme in Home Area Network under Smart Grid system

정 도 영 (丁 度 榮 Chung, Doyoung)

전산학과

Department of Computer Science

KAIST

2012

스마트 그리드 시스템의 댁내망에서 개인정보 보호를 위한 인증 기법 연구

A Study on Privacy-preserving Authentication Scheme
in Home Area Network under Smart Grid system

A Study on Privacy-preserving Authentication Scheme in Home Area Network under Smart Grid system

Advisor : Professor Kwangjo Kim

by

Chung, Doyoung
Department of Computer Science
KAIST

A thesis submitted to the faculty of KAIST in partial fulfillment of the requirements for the degree of in the Department of Computer Science . The study was conducted in accordance with Code of Research Ethics[1].

2011. 12. 20.

Approved by

Professor Kwangjo Kim

[Advisor]

[1] Declaration of Ethical Conduct in Research: I, as a graduate student of KAIST, hereby declare that I have not committed any acts that may damage the credibility of my research. These include, but are not limited to: falsification, thesis written by someone else, distortion of research findings or plagiarism. I affirm that my thesis contains honest conclusions based on my own careful research under the guidance

스마트 그리드 시스템의 댁내망에서 개인정보 보호를 위한 인증 기법 연구

정 도 영

위 논문은 한국과학기술원 석사학위논문으로
학위논문심사위원회에서 심사 통과하였음.

2011년 12월 20일

심사위원장	김광조	(인)
심사위원	박진아	(인)
심사위원	이기혁	(인)

of my thesis advisor.

MCS
20103576

정 도 영. Chung, Doyoung. A Study on Privacy-preserving Authentication Scheme in Home Area Network under Smart Grid system. 스마트 그리드 시스템의 댁내망에서 개인정보 보호를 위한 인증 기법 연구. Department of Computer Science . 2012. 34p. Advisor Prof. Kwangjo Kim. Text in English.

ABSTRACT

The SG (Smart Grid) system provides lots of advantages to its main stakeholders. It cannot only reduce wasted energy and maintenance cost [1], but also increase reliability and transparency while delivering the generated electricity from suppliers to customers. The HAN (Home Area Network), which consists of smart appliances, a SM(Smart meter) and its management system, allows an end-user to control and monitor many digital devices remotely. However, anyone can easily eavesdrop a communication between the components of the HAN due to the wireless communication to support the easy deployment. As a result, an adversary easily identifies which type of appliances belongs to the end-user by monitoring the pattern of the power consumption. On the other hand, there is a possibility that the end-user tries to manipulate his SM. A government may give some advantages to the industry, such as government subsidy for electricity car. This is the reason why the end-user wants to manipulate his SM. Thus we should support an efficient privacy-preserving authentication for HAN. Our protocol supports a variety of security features such as mutual authentication, confidentiality, message integrity, anonymous communication, and resiliency against compromising SM. Our protocol has other strong point such as lightweightness which is of ultimate importance for protocols which perform on HAN, because the core entities for HAN, such as the SM, have only limited computational power. By using our protocol, the end user can get many benefits, such as confirming the amount of the power consumption for each appliance. And the SM can request power to utility provider in advance for efficiency.

Contents

List of Tables

List of Figures

].

Chapter 1. Introduction

1.1 Overview

The SG (Smart Grid) provides big advantages to its main stakeholders (*i.e.,* supplier and end-user). It reduces a wasted energy, CO_2 consumption, maintenance cost and increases reliability with transparency during delivering generated electricity from the power supplier to an end-user. An end-user takes advantages from the SG. One of advantages of the SG is that a customer's appliances can operate when the price of electricity is relatively cheap. By using SG, the electricity suppliers can change the price of electricity depending on the cost of generating electricity. For example, the price of reusable electricity (*i,e.,* solar, wind energy) is set to be cheaper than traditional electricity and the electricity for electricity car is exempted from consumption tax to encourage electricity car maker.

Adopting those special electricity charges may affect the end-user to manipulate his smart meter at home to gain illegal profit. For example, the end-user may disguise his refrigerator to his electricity car to avoid consumption tax.

Although wireless communication is necessary in order to support uninterrupted deployment in HAN(Home Area Network), an adversary can easily obtain the private information of an end-user by eavesdropping (*i.e.,* life style, billing information, existence of an end-user, and appliance types). The usage pattern of electricity at home could lead to disclosure of not only how much energy consumption but also when they are at home, at work, or traveling [2, 3].

In addition, the adversary can compromise the smart meter, because the smart meter is usually located on the outside of the accommodation. Thus, we should provide resiliency against compromising the smart meter.

However, some HAN devices (*e.g.,* smart appliances and smart meter) are limited under a certain level of computing capabilities to keep the running costs down, which may limit the types and layers of security that could be applied for[4]. Thus the authentication protocol for HAN should be lightweight [5].

We also consider a scalability issue of the system. Because the end-user may want to attach (or remove) a new smart appliance in his HAN and replace his smart appliance with new one at his home.

From these observations, the system for HAN is required to achieve the following security requirements; confidentiality, message integrity, mutual authentication, privacy preservation of an end-user, and non-repudiation.

To achieve these security requirements, we use our system model for HAN as Figure 1.1. The management system, such as the home server, can be operated under a ubiquitous environment, whatever services are provided to customers. That is the reason why we include the home server in our system model. In addition, the end-user can remotely control his smart appliances through the home server, and check his electricity bill and the power consumptions of each smart appliance from outside of his accommodation. The smart meter gathers the information such as the power consumption from all smart appliances and reports it to the home server.

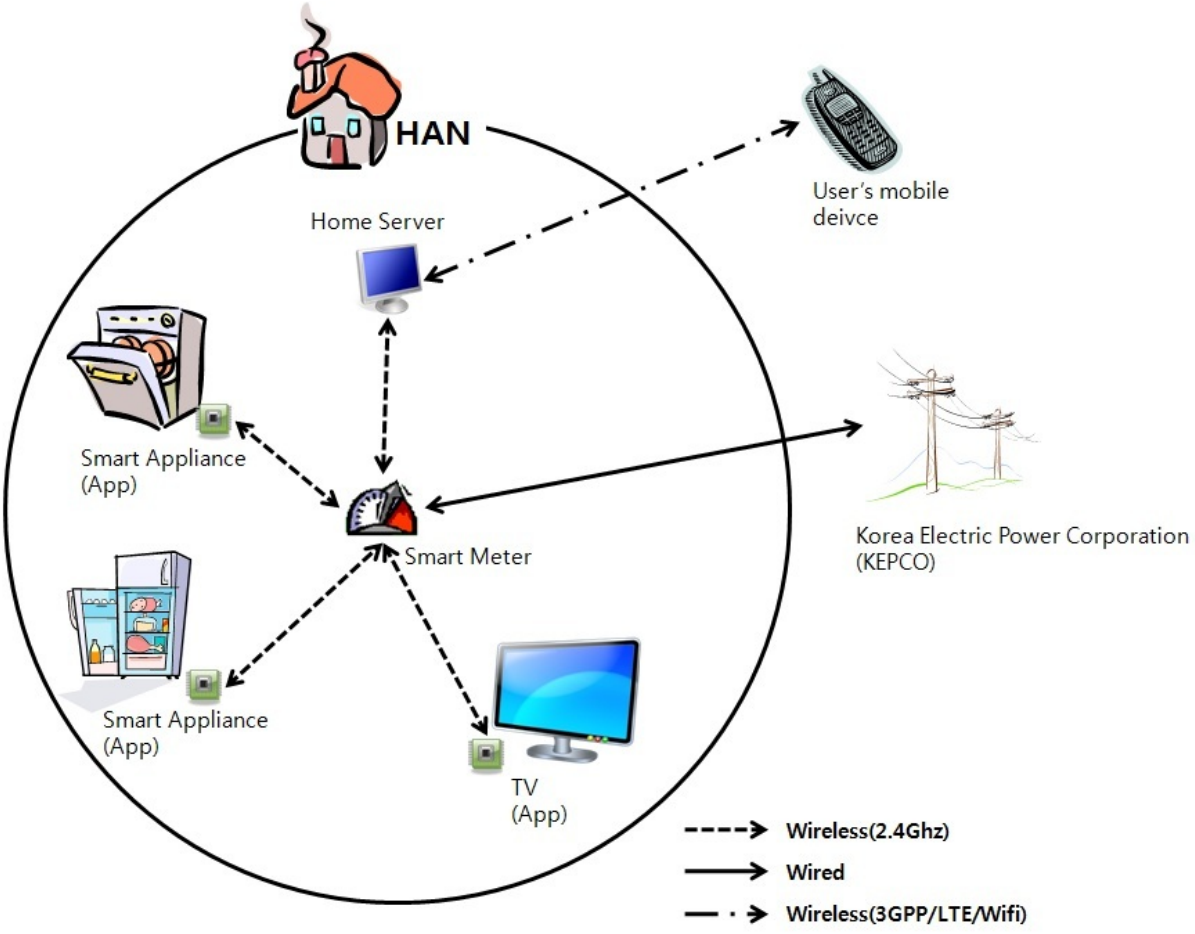


Figure 1.1: Our system model for HAN

In this thesis, we suggest an efficient and privacy-preserving authentication protocol for HAN over the SG which satisfies the security requirements described before.

1.2 Our Contribution

In this thesis, we propose a novel efficient and privacy-preserving authentication scheme in HAN. Our scheme guarantees mutual authentication, confidentiality and integrity, anonymity, and resiliency against compromising smart meter. Also it satisfies lightweightness simultaneously. We utilize the BGN encryption [6] with the membership verification to address the contradictory requirements. Our scheme also use Diffie-Hellman key exchange scheme to register all the smart appliances to the home server. This scheme may require some computational overhead, but the registration phase is performed only once when new appliance has been introduced in the HAN of the end user, which does not require the service time operations. We also introduce new system architecture, as depicted in Figure 1.2. By adopting this system architecture, we can adopt 3rd party escrow service to satisfy our security requirements.

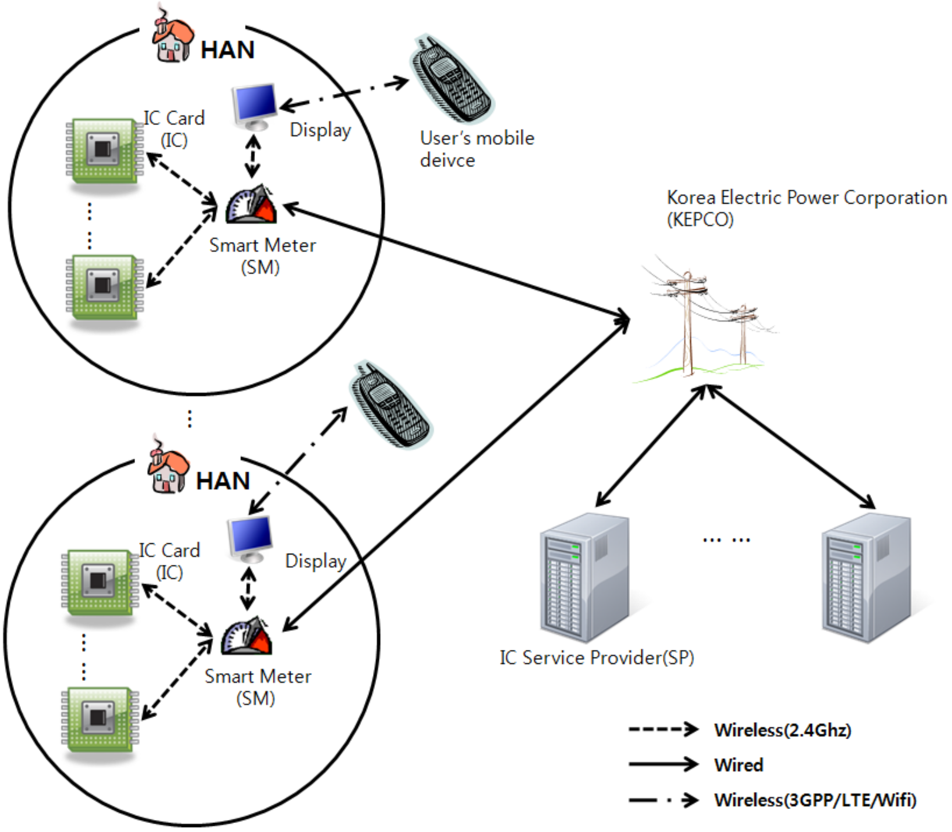


Figure 1.2: Our system architecture

By using our protocol, the end user can confirm the amount of the power consumption for each appliance. Thus, the smart meter can request power to utility provider in advance for efficiency. From the point of the government side, they can enforce a policy that gives advantage for an industry they want to develop without illegal usage by an end user. Our protocol fulfills security requirement, at the same time, it offers user friendly functionalities.

1.3 Organization

The remainder of the thesis is organized as follows: A brief survey on the related work and the background of our work is conducted in Chapter 2. Our authentication scheme is presented in detail in Chapter 3. Chapter 4 analyzes the security and performance of the proposed scheme. Finally, we summarize and conclude the thesis in Chapter 5.

Chapter 2. Background and Related Work

2.1 Related Work

2.1.1 BGN encryption

In 2005, Boneh *et al.* [6] proposed a new homomorphic encryption scheme (denoted as BGN encryption) supporting unlimited additive operations and one multiplicative operation on the encrypted data. The proposed encryption scheme enables one entity to evaluate the encrypted data without revealing the real content of the encrypted data. We review the BGN encryption scheme in brief.

In BGN encryption, all operations are executed over two cyclic group G and G_1 with the same order $n = q_1 q_2$, where q_1 and q_2 are two large prime numbers.

The public key PK_{BGN} is g and $h = g^{\mu q_2}$ under the group G, where μ is a random integer. The encryption of m_i, $m_i + m_j$, and $m_i m_j$ can be computed as $g^{m_i} h^{r_i}$, $g^{m_i} h^{r_i} g^{m_j} h^{r_j}$ and $e(g^{m_i} h^{r_i}, g^{m_j} h^{r_j})$, $m_i \in Z_T$ be i-th message, where T is a non-zero random number less than q_2, r_i is i-th random number, and e is a bilinear mapping from $G \times G$ to G_1. The expected decryption time using Pollard's lambda method [7] is $\tilde{O}(\sqrt{|T|})$ although the authentication server has the private key, $SK_{BGN} = q_1$.

2.1.2 Membership verification

In 2008, Yau *et al.* [8] proposed an idea to convert the searching of the sets to an evaluation of polynomial representations of a given set [9, 10] using BGN encryption [6].

However, the proposed approach is not efficient from the view of computational overhead. Denote S_1 and S_2 by a set of access keys and a set of keywords, respectively. Then, the end-user should compute $(|S_1| + |S_2| + 1)$ exponent multiplications and BGN encryptions per each query.

To reduce the computational overhead, Kim *et al.* [11] revised the definition of the polynomial presenting the sets and proposed new verification algorithm. The end-user should compute $(|S_2| + 1)$ BGN encryptions per each query. Also, Kim *et al.* suggested an idea to reduce the verification cost while providing a certain level of performance. Although this approach is more lightweight than the scheme proposed by Yau *et al.* [8], the membership verifier should perform some pairing computations and exponent multiplications. Note that the number of pairing computations and exponent multiplications is a crucial factor to determine the desired performance.

2.1.3 Undetectable Appliance Load Signatures

In 2010, Georgios *et al.* [12] proposed a method that moderates the pattern of the power consumption of a house, thus hides power consumption of each appliance from an adversary. Their work introduced an algorithm which mixes the usage pattern of electricity. This algorithm is based on a power management model which is used for a rechargeable battery. They argued that privacy can be protected by supplying power from the rechargeable battery rather than from electricity grid directly.

They proved that their proposal has protected privacy of the end user well, but there were some limitations. The privacy protection level is proportional to the capacity of the rechargeable battery and the users have to pay an extra cost to buy the rechargeable battery. Moreover, the security requirements which protect user privacy may conflict with the other requirements (such as cost-saving from energy pricing arbitrage)[12].

2.1.4 Privacy via anonymization of smart metering data

In 2010, Efthymiou *et al.* [13] proposed a protocol that protects privacy of the end user via anonymization of smart metering data. The smart metering data is separated into two parts; high-frequency data and low-frequency data. The high-frequency data is the consumption of power for each smart appliance which is reported every few minutes. The low-frequency data is related with billing and includes privacy data of the end user. These data usually reported every week or month.

They also aimed to fulfill the lightweightness of their protocol which guarantees anonymization of smart metering data. They used the third party escrow based on anonymization to avoid a leakage of personal information of the user.

However, their protocol neither considers the possibility of tampering the smart meter by user, nor supports an authentication between the smart meter and the smart appliance or the electricity vehicle.

2.1.5 Privacy-Preserving Smart Metering

In 2010, Rial *et al.* [14] have proposed a suite of protocols amongst a provider, a user and a tamper-evident meter. In this protocol, the system model consists of the smart meter, user device or service, and the provider. They introduce a term which called policy. A policy is a kind of functions that the input is the power consumption for a specific interval, and other information which is necessary to calculate the electricity bill. For example, a time of usage of an appliance can be the other information if the price of power depends on when it has been used. The provider can be modeled as a utility provider, such as KEPCO in Korea, determines a policy.

The user device gains information of the power consumption for the specific interval from the smart meter. The user device calculates the price of electricity for specific interval based on the information from the smart meter and other information, such as, the amount of the previous power consumption. The user device sends the price of electricity for specific interval to the provider.

While exchanging the data and calculated price of electricity for specific interval, the authentication and the reliability of data is guaranteed by public key signature scheme. The privacy of a user can be preserved because the data related with privacy of the end user, such as the power consumption for each device, must be revealed only to the provider, but not to the smart meter. Even though an adversary can manipulate the smart meter, he cannot gain the data related with privacy of the end user.

However, there are some limitations for this thesis. First, it uses public key signature scheme for communication. It supports the authentication and guarantees the reliability, but the public key signature scheme is too burden for smart meter in general. The suggested system model is quite different from ongoing smart grid projects as they restrict direct communication between the metering core and the provider to protect privacy [14]. For these reasons, we have changed lots of part of an infrastructure of power grid to apply this protocol to the real practice.

Chapter 3. Our Scheme

3.1 Security Requirements

3.1.1 Mutual authentication

Although the wireless communication is necessary in order to support easy deployment in HAN, an adversary can disguise itself as an IC card to other entities. It occurs a serious problem, for example, the end user is forced to pay for electricity which he has never used. An entity which participates in communication should confirm a message is also sent by a proper entity, because each message includes the critical private information such as the social security number of an end user. Thus message authentication should be provided to protect message forgery and related attacks.

3.1.2 Confidentiality and Integrity

All messages should be securely transfered to a legitimate receiver. For example, a message that is sent by an electricity vehicle should be sent to only a smart meter which provides electricity to the electricity vehicle.

The information of the critical and sensitive message, such as the power consumption of an appliance, *etc.* is directly related with bills. Some types of message should be handled in the real-time. The power request message is an example which should be handled in the real-time. A message includes critical information such as the power consumption of each appliance, the social security number of an end user, *etc.* If the message has been modified, it occurs serious problems, such as, the electricity bill is sent to a wrong end user. Thus the integrity of message must be guaranteed.

3.1.3 Anonymity

The messages contains the privacy-related data, such as the location of smart meter, the owner of credit card used for payment, an adversary can identify which electrical appliances are used and the amount of power the electrical appliances are used through load monitoring [15, 16]. As a result, detailed consumption data would facilitate the creation of lifestyle profile of users with information, such as when they are at home, when they eat, whether they arrive late to work, *etc.*

To avoid those vulnerabilities, our protocol interrupts load monitoring by the adversary and hides the identity of user from the adversary. Whenever the smart meter or an IC card sends information to KEPCO or SP, it will send only the least information for operations.

3.1.4 Resiliency against compromising smart meter

The smart meter is usually located outside of an accommodation. Thus, it inherently is vulnerable to physical compromising. By compromising smart meter, session keys stored in the smart meter may be exposed to an adversary. Even if the session keys are exposed to the adversary, our protocol should protect the private information of end users.

On the other hand, an end user also wants to compromise smart meter. A government expected to give tariff advantages for the industry which it wants to develop. Especially, in Korea, a cumulative policy is accepted for electricity bills and it is expected that the Korean government except electricity vehicles from the cumulative policy rather than linear policy. Thus the end user has economical motivation to compromise the smart meter, and our protocol should provide prevention against compromising smart meter by the end user.

3.2 Our membership verification

We convert membership verification to set search by evaluating of a polynomial representing a given set [9, 10], where the set contains the service subscriber lists. Compared to the membership verification of the previous work [11], our membership verification is reduced only one exponent operation. From this respect, we argue that our membership verification can be one of efficient approaches.

3.2.1 Assumption

We assume that whenever a SP is registered to KEPCO, it sends KEPCO a token verifier for itself, $E[-(\alpha-1)r, PK_{BGN}, G]$. Also the key agreement between the SP and KEPCO is performed. Thus KEPCO can find out appropriate SP using our membership verification and the communication between KEPCO and the SP is secure.

Also when the smart meter is installed in the house of end user, the key agreement between the home server and the smart meter, and the smart meter and KEPCO is performed. And the nonces for communication between the home server and the smart meter, and the smart meter and KEPCO are generated. Thus the communication between the home server and the smart meter, and the smart meter and KEPCO must be secure.

And we assume that the IC is tamper resistant. A session key between the IC and the SP, and nonce for communication between the IC and the SP is embedded when the IC is produced.

3.2.2 Polynomial generation

For a set $S_1 = \{w_1, w_2, \cdots, w_p\}$, a polynomial with degree t, $f(x)$ is defined as

$$f(x) = \begin{cases} E[-\alpha r, PK_{BGN}, G] & x = w_i \in S_1 \\ E[-r', PK_{BGN}, G] & x = w_i \notin S_1, \end{cases}$$

where α, r, and $r'(r' \neq r)$ are random integers. Here, $w_i = E[-r', PK_{BGN}, G] = g^{-r}h^{R_i}$ is an authorized token of *i-th* appliance.

Given $x_i \in S_i = E[-r', PK_{BGN}, G]$ & $f(x) = x \times E[-(\alpha - 1)r, PK_{BGN}, G]$,

then, $f(x_i) = x_i \times E[-(\alpha - 1)r, PK_{BGN}, G] = E[-\alpha r, PK_{BGN}, G]$

Above equation presents an example of generating a polynomial. If the appliance exists in the set, the evaluation result of the given polynomial $f(x)$ is a fixed value $E[-\alpha r, PK_{BGN}, G]$ where r is 0 to $2^{160} - 1$. Therefore, we can verify whether the end-user exists in the subscriber list.

3.2.3 Polynomial evaluation

For membership verification, an appliance submits w_i to the membership verifier (*i.e.,* smart meter). Then, the membership verifier checks whether the appliance belongs to one of the appliances of the end user by computing $f(w_i)$. Only if $f(w_i) = -\alpha r$, the appliance is a legitimate one.

However, we want to hide the detailed information of membership function from the adversary. That's why the membership verifier performs the following steps:

$(S1) Compute\ C = w_i \times E[-(\alpha - 1)r, PK_{BGN}, G]$

$(S2) Compare\ C^{SK_{BGN}}\ with\ the\ stored\ g^{-\alpha r \cdot SK_{BGN}}$

3.3 Our protocol

Guidelines for Smart Grid Cyber Security published by NIST [3] says that, “Due to the relatively new technologies used in HANs, communication protocols have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing.”

Moreover, the smart meter in HAN can be compromised by the adversary. The device is exposed to physical security issues such as a poor maintenance, misusage, and theft.

Our protocol consists of six phases; appliance registration, appliance authentication, token reissue, token change, power request, and report. In the following, we describe our protocol in detail. Hereinafter IC, HS, SM, SP, and KEPCO correspond to an IC card, a home server, a smart meter, a service provider and Korea Electric Power Corporation. $H(m)$ notates that a hash value of message m using a hash function such as SHA-1 and $E\{m, K_A\}$ notates that a encrypted message of message m by a symmetric key K_A.

3.3.1 Appliance registration phase

Through the appliance registration phase, a HS and an IC perform key agreement by Diffie-Hellman key exchange and the HS sends a session key for the IC and a SM. Figure 3.1 shows the appliance registration phase.

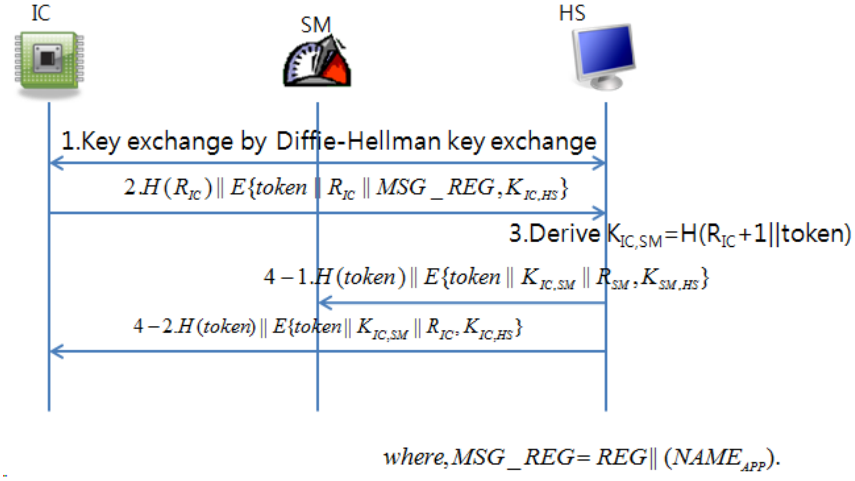

IC
SM
HS
1.Key exchange by Diffie-Hellman key exchange
$2.H(R_{IC}) \| E\{token \| R_{IC} \| MSG\_REG, K_{IC,HS}\}$
3.Derive $K_{IC,SM}=H(R_{IC}+1\|token)$
$4-1.H(token) \| E\{token \| K_{IC,SM} \| R_{SM}, K_{SM,HS}\}$
$4-2.H(token) \| E\{token \| K_{IC,SM} \| R_{IC}, K_{IC,HS}\}$
$where, MSG\_REG = REG \| (NAME_{APP}).$

Figure 3.1: Appliance registration

Through the appliance registration phase, a HS and an IC perform key agreement by Diffie-Hellman key excahnge. After key agreement, the IC requests the HS to register itself with its token and nonce,

R_{IC}. R_{IC} is generated by the IC during this phase. The HS generates session key between the IC and a SM, $K_{IC,SM}$, based on R_{IC} and the token belongs to the IC. The HS sends $K_{IC,SM}$ to the SM and the IC. As we assume in section 3.2.1, the session key between the HS and the SM has already been agreed. And the session key between the HS and the IC have already been agreed during this phase, thus $K_{IC,SM}$ can be sent securely. The detail of this phase is decribed as below.

1.IC ↔ HS: Key exchange by Diffie-Hellman key exchange

2.IC → HS: $H(R_{IC})||E\{token||R_{IC}||MSG\_REG, K_{IC,HS}\}$

3.HS: Derive $K_{IC,SM} = H(R_{IC} + 1||token)$

4-1.HS → SM: $H(token)||E\{token||K_{IC,SM}||R_{SM}, K_{SM,HS}\}$

4-2.HS → IC: $H(token)||E\{token||K_{IC,SM}||R_{IC}, K_{IC,HS}\}$

3.3.2 Appliance authentication phase

During appliance authentication phase, the appliance is authenticated to KEPCO and SP simultaneously. The SP confirm whether the appliance is appropriate or not by R'_{IC} and $K_{IC,SP}$. R'_{IC} and $K_{IC,SP}$ is hardcoded to the IC when the IC is manufactured, thus only the message which generated by proper IC can be encrypted by $K_{IC,SP}$ and contains proper R'_{IC}. Through membership verification discussed in Section 3, KEPCO can find out suitable SP by our membership verification scheme with token, $E[-r, PK_{BGN}, G]$. Only if the computed result $C^{SK_{BGN}}$ is the same as the stored one in the memory, KEPCO can trust the appliance belongs to a membership which correspond to $C^{SK_{BGN}}$. In our membership verification, the entity which has token verifier, $E[-(\alpha-1)r, PK_{BGN}, G]$, can confirm whether the entity belongs to the membership or not by one exponent multiplication and one exponent addition. The number of membership is not quite large and KEPCO has strong computational power, thus the work to find out the proper membership for each IC is not burden for KEPCO. Moreover the token doesn't have any identity about the IC, but only can be used to confirm the entity belongs to the membership or not.

By this process, KEPCO and SP can trust that the message is sent by proper IC. And as we assume in Section 1, the IC is tamper resistant. Thus KEPCO and SP can rule out the possibility of manipulating message by an end user. This phase is shown in 3.2 and we decribe the detail of this phase as below.

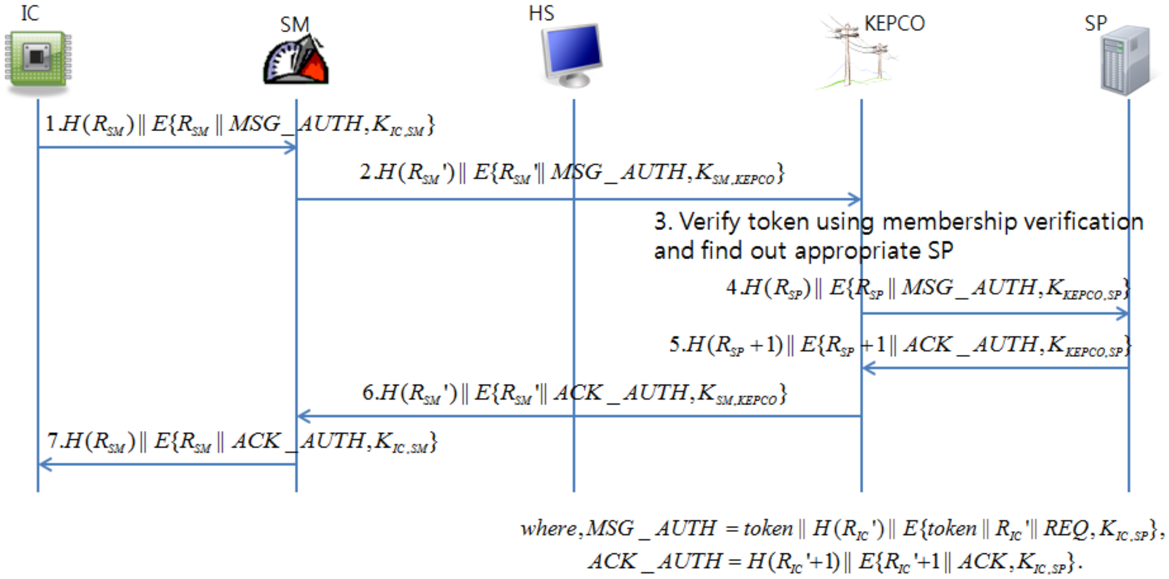

IC
SM
HS
KEPCO
SP
$1.H(R_{SM}) \| E\{R_{SM} \| MSG\_AUTH, K_{IC,SM}\}$
$2.H(R_{SM}') \| E\{R_{SM}' \| MSG\_AUTH, K_{SM,KEPCO}\}$
3. Verify token using membership verification and find out appropriate SP
$4.H(R_{SP}) \| E\{R_{SP} \| MSG\_AUTH, K_{KEPCO,SP}\}$
$5.H(R_{SP}+1) \| E\{R_{SP}+1 \| ACK\_AUTH, K_{KEPCO,SP}\}$
$6.H(R_{SM}') \| E\{R_{SM}' \| ACK\_AUTH, K_{SM,KEPCO}\}$
$7.H(R_{SM}) \| E\{R_{SM} \| ACK\_AUTH, K_{IC,SM}\}$
$where, MSG\_AUTH = token \| H(R_{IC}') \| E\{token \| R_{IC}' \| REQ, K_{IC,SP}\},$
$ACK\_AUTH = H(R_{IC}'+1) \| E\{R_{IC}'+1 \| ACK, K_{IC,SP}\}.$

Figure 3.2: Appliance authentication

1.IC → SM: $H(R_{SM})||E\{R_{SM}||MSG\_AUTH, K_{IC,SM}\}$

2.SM → KEPCO: $H(R'_{SM})||E\{R'_{SM}||MSG\_AUTH, K_{SM,KEPCO}\}$

3.KEPCO: Verify token using membership verification and find out appropriate SP

4.KEPCO → SP: $H(R_{SP})||E\{R_{SP}||MSG\_AUTH, K_{KEPCO,SP}\}$

5.SP → KEPCO: $H(R_{SP}+1)||E\{R_{SP}+1||ACK\_AUTH, K_{KEPCO,SP}\}$

6.KEPCO → SM: $H(R'_{SM})||E\{R'_{SM}||ACK\_AUTH, K_{SM,KEPCO}\}$

7.SM → IC: $H(R_{SM})||E\{R_{SM}||ACK\_AUTH, K_{IC,SM}\}$

3.3.3 Token reissue phase

There is a possibility that an adversary guesses the relationship between token and appliance, if the end user has been using their tokens for the long period. To avoid this threat, our protocol has to change token periodically. To support this operation, SP reissues token which $E[-r, PK_{BGN}, G]$. KEPCO already has verifier for this token, $E[-(\alpha-1)r, PK_{BGN}, G]$. Thus KEPCO recognizes which token belongs to which SP without any change for their token verifiers. The new token is sent to the IC safely by using session key between IC and SP. We describe this phase more detail in Figure 3.3

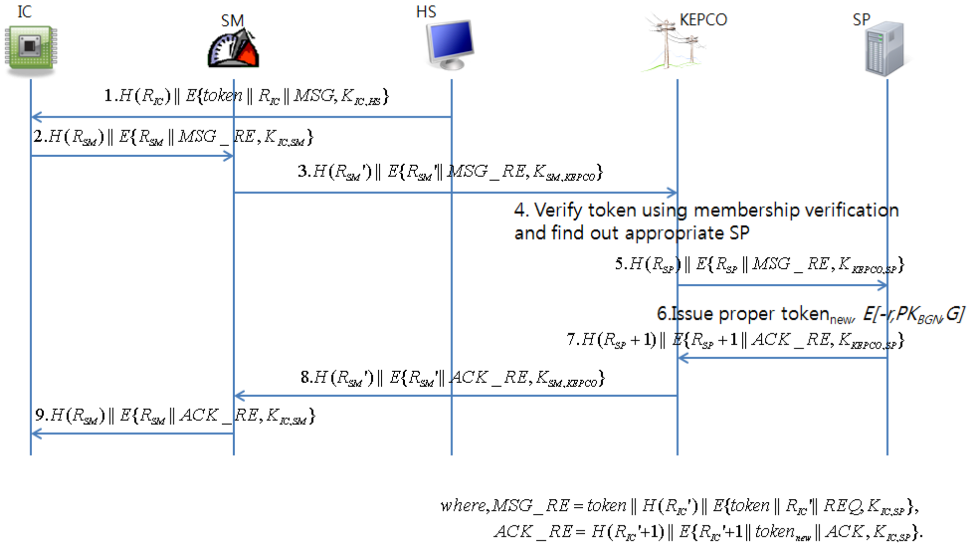

IC
SM
HS
KEPCO
SP
1.$H(R_{IC}) \| E\{token \| R_{IC} \| MSG, K_{IC,HS}\}$
2.$H(R_{SM}) \| E\{R_{SM} \| MSG\_RE, K_{IC,SM}\}$
3.$H(R_{SM}') \| E\{R_{SM}' \| MSG\_RE, K_{SM,KEPCO}\}$
4. Verify token using membership verification and find out appropriate SP
5.$H(R_{SP}) \| E\{R_{SP} \| MSG\_RE, K_{KEPCO,SP}\}$
6.Issue proper token$_{new}$, $E[-r, PK_{BGN}, G]$
7.$H(R_{SP}+1) \| E\{R_{SP}+1 \| ACK\_RE, K_{KEPCO,SP}\}$
8.$H(R_{SM}') \| E\{R_{SM}' \| ACK\_RE, K_{SM,KEPCO}\}$
9.$H(R_{SM}) \| E\{R_{SM} \| ACK\_RE, K_{IC,SM}\}$
where, $MSG\_RE = token \| H(R_{IC}') \| E\{token \| R_{IC}' \| REQ, K_{IC,SP}\}$,
$ACK\_RE = H(R_{IC}'+1) \| E\{R_{IC}'+1 \| token_{new} \| ACK, K_{IC,SP}\}$.

Figure 3.3: Token reissue

The detail of this phase is described as below.

1.HS → IC: $H(R_{IC})||E\{token||R_{IC}||MSG, K_{IC,HS}\}$

2.IC → SM: $H(R_{SM})||E\{R_{SM}||MSG\_RE, K_{IC,SM}\}$

3.SM → KEPCO: $H(R'_{SM})||E\{R'_{SM}||MSG\_RE, K_{SM,KEPCO}\}$

4.KEPCO: Verify token using membership verification and find out appropriate SP

5.KEPCO → SP: $H(R_{SP})||E\{R_{SP}||MSG\_RE, K_{KEPCO,SP}\}$

6.SP: Issue proper $token_{new}$, $E[-r, PK_{BGN}, G]$

7.SP → KEPCO: $H(R_{SP}+1)||E\{R_{SP}+1||ACK\_RE, K_{KEPCO,SP}\}$

8.KEPCO → SM: $H(R'_{SM})||E\{R'_{SM}||ACK\_RE, K_{SM,KEPCO}\}$

9.SM→ IC: $H(R_{SM})||E\{R_{SM}||ACK\_RE, K_{IC,SM}\}$

3.3.4 Token change phase

The HS sends order for token change to the IC. Then, the IC sends new token which has already been reissued by the SP. The HS generates a new session key for IC and SM by using the new token and sends it to the SM and IC. During this phase, the SM receives only new token and the new session key pair, and it does not have information related with the old token and new token. KEPCO and SP has the old token and new token pair, thus reauthentication between IC and SP is not required. This phase is shown in Figure 3.4.

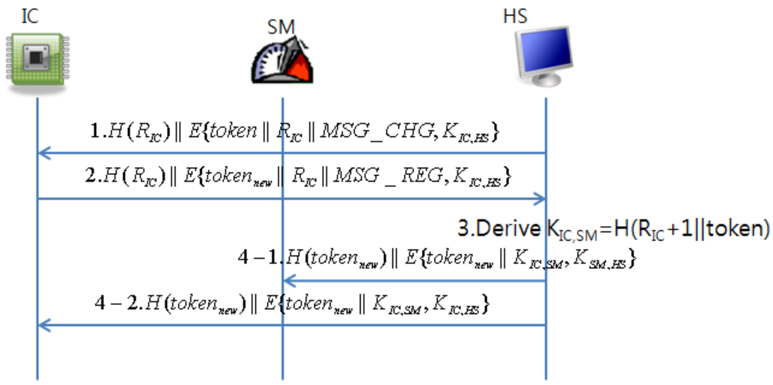

IC
SM
HS
$1.H(R_{IC}) \| E\{token \| R_{IC} \| MSG\_CHG, K_{IC,HS}\}$
$2.H(R_{IC}) \| E\{token_{new} \| R_{IC} \| MSG\_REG, K_{IC,HS}\}$
3.Derive $K_{IC,SM}$=H(R_{IC}+1||token)
$4-1.H(token_{new}) \| E\{token_{new} \| K_{IC,SM}, K_{SM,HS}\}$
$4-2.H(token_{new}) \| E\{token_{new} \| K_{IC,SM}, K_{IC,HS}\}$

Figure 3.4: Token change

The detail of this phase is described as below.

1.HS → IC: $H(R_{IC})||E\{token||R_{IC}||MSG\_CHG, K_{IC,HS}\}$

2.IC → HS: $H(R_{IC})||E\{token_{new}||R_{IC}||MSG\_REG, K_{IC,HS}\}$

3.HS: Derive $K_{IC,SM} = H(R_{IC} + 1)||token)$

4-1.HS → SM: $H(token_{new})||E\{token_{new}||K_{IC,SM}, K_{SM,HS}\}$

4-2.HS → IC: $H(token_{new})||E\{token_{new}||K_{IC,SM}, K_{IC,HS}\}$

3.3.5 Power request phase

The appliance sends a request to deal with the expected electronic power consumption in a certain time period. Then, the SM verifies the received request, reserves proper power, and sends result to the appliance if only the verification result is correct. Figure 3.5 depicts the power request phase.

Although the end-user leaves his accommodation without plugging the unused appliances, our protocol can minimize an unnecessary power consumption of the unused appliances by adopting the time period. Our protocol also supports for special billing type such as government aided bill for electricity car. By using the membership verification with the token, KEPCO can forward power request message to appropriate SP. To avoid the illegal uses by manipulating SM, the SP check validity of the message by token and requests the end-user to pay by various way, such as, credit card, bill, transfer, *etc.* The SP notices KEPCO whether payment is done or not. KEPCO sends power to the appliance only when

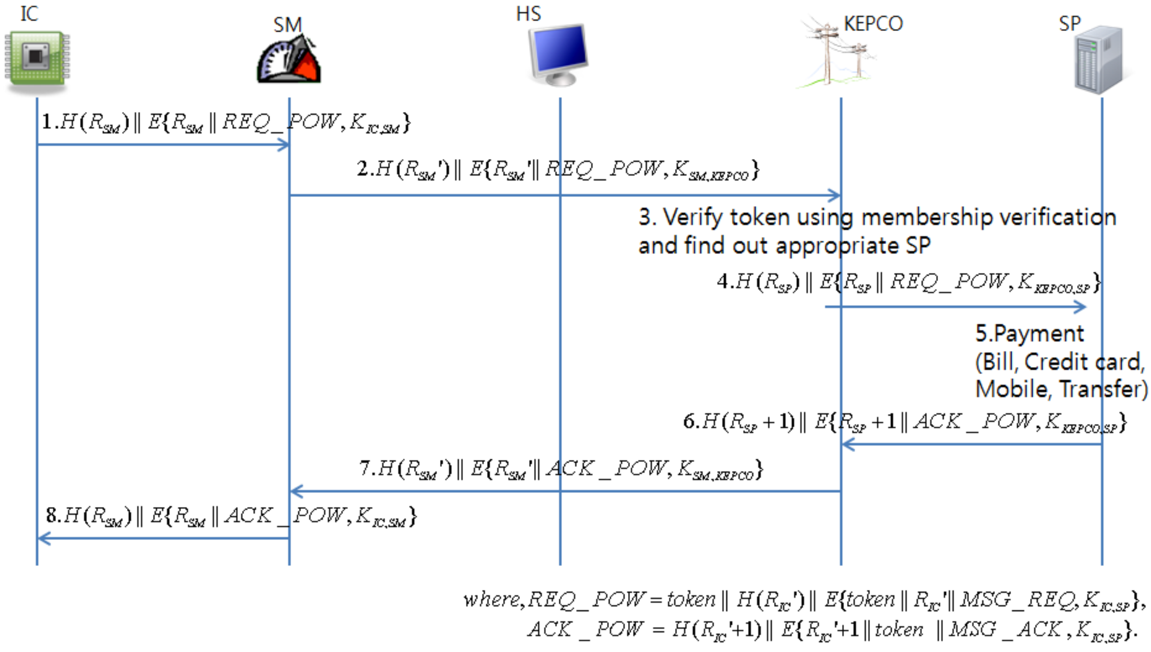

IC
SM
HS
KEPCO
SP
$1.H(R_{SM}) \| E\{R_{SM} \| REQ\_POW, K_{IC,SM}\}$
$2.H(R_{SM}') \| E\{R_{SM}' \| REQ\_POW, K_{SM,KEPCO}\}$
3. Verify token using membership verification and find out appropriate SP
$4.H(R_{SP}) \| E\{R_{SP} \| REQ\_POW, K_{KEPCO,SP}\}$
5.Payment (Bill, Credit card, Mobile, Transfer)
$6.H(R_{SP}+1) \| E\{R_{SP}+1 \| ACK\_POW, K_{KEPCO,SP}\}$
$7.H(R_{SM}') \| E\{R_{SM}' \| ACK\_POW, K_{SM,KEPCO}\}$
$8.H(R_{SM}) \| E\{R_{SM} \| ACK\_POW, K_{IC,SM}\}$
$where, REQ\_POW = token \| H(R_{IC}') \| E\{token \| R_{IC}' \| MSG\_REQ, K_{IC,SP}\},$
$ACK\_POW = H(R_{IC}'+1) \| E\{R_{IC}'+1 \| token \| MSG\_ACK, K_{IC,SP}\}.$

Figure 3.5: Power request

the payment is done appropriately.

The detail of this phase is described as below.

1.IC → SM: $H(R_{SM})||E\{R_{SM}||REQ\_POW, K_{IC,SM}\}$

2.SM → KEPCO: $H(R'_{SM})||E\{R'_{SM}||REQ\_POW, K_{SM,KEPCO}\}$

3.KEPCO: Verify token using membership verification and find out appropriate SP

4.KEPCO → SP: $H(R_{SP})||E\{R_{SP}||REQ\_POW, K_{KEPCO,SP}\}$

5.SP: Payment(Bill, Creidt card, Mobile, Transfer)

6.SP → KEPCO: $H(R_{SP}+1)||E\{R_{SP}+1||ACK\_POW, K_{KEPCO,SP}\}$

7.KEPCO → SM: $H(R'_{SM})||E\{R'_{SM}||ACK\_POW, K_{SM,KEPCO}\}$

8.SM→ IC: $H(R_{SM})||E\{R_{SM}||ACK\_POW, K_{IC,SM}\}$

3.3.6 Report phase

Since the end-user may want to observe the status of energy consumption, the HS should collect the electronic power consumption from the SM.

The HS sends the request for collecting the electronic power consumption of an appliance to the

SM. This message is encrypted by the session key, $K_{SM,HS}$. Only when the received R_{HS} is same as the stored nonce for the HS in the memory, the SM sends acknowledge message to the HS.

Since token is used to identify the target IC, the SM cannot identify what the IC is. In next paper, we describe this phase in Figure 3.6

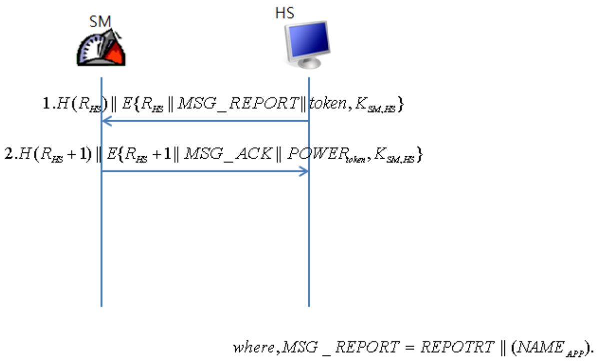

SM
HS
$1.H(R_{HS})\|E\{R_{HS}\|MSG\_REPORT\|token, K_{SM,HS}\}$
$2.H(R_{HS}+1)\|E\{R_{HS}+1\|MSG\_ACK\|POWER_{token}, K_{SM,HS}\}$
$where, MSG\_REPORT = REPOTRT \| (NAME_{APP}).$

Figure 3.6: Report

The detail of this phase is described as below.

1.HS → SM: $H(R_{SM})||E\{R_{SM}||MSG\_REPORT||token, K_{SM,HS}\}$

2.SM → HS: $H(R_{SM}+1)||E\{R_{SM}+1||MSG\_ACK||POWER_{token}, K_{SM,HS}\}$

Chapter 4. Security and Performance Analysis

4.1 Performance Analysis

Our goal is to use of commercial application, and it has to balance between strength of security and performance. To satisfy this purpose, the size of keys or nonce in our protocol may be decided to provide the commercial level of security. For example, we use 128 bit key for symmetric encryption which follows the guidelines of NIST [3]. In Table 4.1, we define the size of nonce, symmetric key, keys for BGN encryption [6], *etc.*

Table 4.1: Storage Requirement

Nonce	64-bit
Symmetric Key	128-bit
$E[-r, PK_{BGN}, G]$	512-bit
$E[-(\alpha-1)r, PK_{BGN}, G]$	512-bit
PK_{BGN}	512-bit
SK_{BGN}	512-bit
Name of Appliance	1024-bit
Power Consumption	32-bit

4.1.1 Storage Overhead

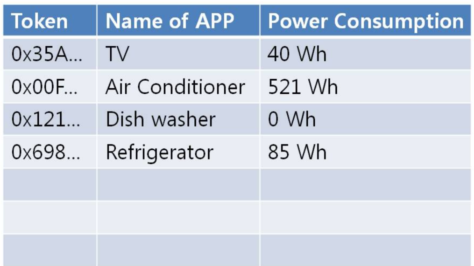
Each entity requires storage to save persistent data or temporarily data for computaition. This overhead is naturally proportional to the number of bits of each saved data. Thus we measure this overhead by count the number of bits required to save each data.

The appliance has to store R_{IC}, R_{SM}, R'_{IC}, $K_{IC,SM}$, $K_{IC,SP}$ and 2 tokens. As listed in Table 4.1, the nonce R_{IC}, R_{SM}, and R'_{IC} requires 64-bit per each. $K_{IC,SM}$, and $K_{IC,SP}$ requires 128-bit per each and token requires 512-bit. Thus, $64 + 64 + 64 + 128 + 128 + 512 + 512 = 1472(bit)$ of space is required for an appliance.

The SM has to store R_{HS}, R'_{SM}, $K_{SM,HS}$ and $K_{SM,KEPCO}$. Moreover, the SM has to store R_{SM} and $K_{IC,SM}$ and token per each appliance. The SM requires $64+64+128+128 = 384(bit)$ and $64+128+512 =$

$704(bit)$ per each appliance. Thus, the total amount of bits required is $384(bit) + 704(bit) \times (the\ number\ of\ appliances)$.

The HS has to store R_{IC}, $K_{IC,HS}$, $K_{SM,HS}$, token, a name of appliance, and a power consumption per each appliance as depicted in Figure 4.1. The HS requires $64 + 64 + 128 + 128 + 512 + 1024 + 32 = 1888(bit)$ per each appliance. Thus, the total amount of bits required is $64 + 1888(bit) \times (the\ number\ of\ appliances)$, because R_{HS} is additionally required for communication between the SM and the HS.



Token	Name of APP	Power Consumption
0x35A...	TV	40 Wh
0x00F...	Air Conditioner	521 Wh
0x121...	Dish washer	0 Wh
0x698...	Refrigerator	85 Wh

Figure 4.1: Memory table of Home Server

KEPCO and the SP also require space to store, R'_{SM}, R_{SP}, $K_{SM,KEPCO}$, $K_{KEPCO,SP}$, R'_{IC}, and token for each entity. However KEPCO and the SP have very large computational power and storage. Thus storage overhead does not affect KEPCO or the SP meaningfully.

4.1.2 Computational Cost

The computational cost of our protocol is as described in Table 4.2, Table 4.3 and Table 4.4. In Table 4.2, the communicational cost for each phase is described in form of the number of hash operations. Similarly, In Table 4.3 and Table 4.4, the communicational cost for each phase is described in form of the number of symmetric key operations or the number of exponent multiplications. If such operation is not required in the phase, we notate it as -. And if such operation is not performed by any entity, we omit such phase from the Table.

Appliance registration phase

In appliance registration phase, the HS and the IC do key exchange by Diffie-Hellman key exchange algorithm. This algorithm is quiet burden for the IC, but appliance registration phase is only performed once and it does not require real time strictly. Thus, this operation is tolerable for the HS and the IC.

The IC computes two hashing and two symmetric key operations to send and receive messages. The

Table 4.2: Computational Cost(Hash)

	IC	SM	HS	KEPCO	SP
Appliance Registration	2	1	3	-	-
Appliance Authentication	4	4	-	2	4
Token Reissue	4	4	-	2	4
Token Change	3	1	3	-	-
Power Request	4	4	-	2	4
Report	-	2	2	-	-

Table 4.3: Computational Cost(Symmetric key operation)

	IC	SM	HS	KEPCO	SP
Appliance Registration	2	1	2	-	-
Appliance Authentication	4	4	-	2	2
Token Reissue	4	4	-	2	2
Token Change	3	1	3	-	-
Power Request	4	4	-	2	2
Report	-	2	2	-	-

Table 4.4: Computational Cost(Exponent Multiplication)

	IC	SM	HS	KEPCO	SP
Appliance Authentication	-	-	-	1	-
Token Reissue	-	-	-	1	2
Power Request	-	-	-	1	-

Table 4.5: Computational Cost(Exponent Addition)

	IC	SM	HS	KEPCO	SP
Appliance Authentication	-	-	-	1	-
Token Reissue	-	-	-	1	1
Power Request	-	-	-	1	-

SM only require one hash and one symmetric key operation for $H(token)||E\{token||K_{IC,SM}, K_{SM,HS}\}$. The HS computes two hash and two symmetric key operations to receive message from the IC, and send message to the IC and the SM. It requires another one hashing to derive $K_{IC,SM}$.

Thus during the appliance registration phase, the IC do one Diffie-Hellman key exchange, two hash operations and two symmetric key operations. The SM does one hash operation and one symmetric key operation. And the HS does one Diffie-Hellman key exchnage, three hash operations and two symmetric key operations.

Appliance authentication phase

In appliance authentication phase, the IC computes one hash and one symmetric key operation to generate $token||H(R'_{IC})||E\{token||R'_{IC}||REQ, K_{IC,SP}\}$, and one hash and one symmetric key operation is additionally required to generate $H(R_{SM})||E\{R_{SM}||MSG\_AUTH, K_{IC,SM}\}$. To receive $H(R_{SM})||E\{R_{SM}||ACK\_AUTH, K_{IC,SM}\}$, the IC computes two hash and two symmetric key operations additionally. Thus, the IC computes four hash and four symmetric key operations during appliance authentication phase.

The SM has to compute two hash and two symmetric key operation to generate $H(R_{SM'})||E\{R_{SM'}||MSG\_AUTH, K_{SM,KEPCO}\}$. One hash and one symmetric key operation is required to reveal MSG_AUTH from $H(R_{SM})||E\{R_{SM}||MSG\_AUTH, K_{IC,SM}\}$, and one hash and one symmetric key operation is additionally required to generate $H(R_{SM'})||E\{R_{SM'}||MSG\_AUTH, K_{SM,KEPCO}\}$ using revealed MSG_AUTH. Similarly, the SM has to compute two hash and two symmetric key operations to receive $H(R_{SM'})||E\{R_{SM'}||ACK\_AUTH, K_{SM,KEPCO}\}$ and send $H(R_{SM})||E\{R_{SM}||ACK\_AUTH, K_{IC,SM}\}$. Thus, the SM computes four hash and four symmetric key operations during appliance authentication phase.

When KEPCO receives $H(R_{SM'})||E\{R_{SM'}||MSG\_AUTH, K_{SM,KEPCO}\}$, it has to compute one hash and one symmetric key operation to reveal $token||H(R'_{IC})||E\{token||R'_{IC}||REQ, K_{IC,SP}\}$. And by using our membership verification scheme, KEPCO find out a proper SP which receives MSG_AUTH. During our membership verification scheme, one exponent multiplication and one exponent addition is required. It has to compute one hash and one symmetric key operation to generate $H(R_{SP})||E\{R_{SP}||MSG\_AUTH, K_{KEPCO,SP}\}$ additionally. Similarly, it has to compute additional two hash and two symmetric key operations to receive $H(R_{SP}+1)||E\{R_{SP}+1||ACK\_AUTH, K_{KEPCO,SP}\}$ and send $H(R_{SM'})||E\{R_{SM'}||ACK\_AUTH, K_{SM,KEPCO}\}$ to the SM. KEPCO computes two hash operations, two symmetric key operations, and one exponent multiplication and one exponent addition during appliance authentication phase.

The SP has to compute two hash and two symmetric key operations to reveal information included in

$H(R_{SP})||E\{R_{SP}||MSG\_AUTH, K_{KEPCO,SP}\}$, and two hash and two symmetric key operations to generate ACK_AUTH and $H(R_{SP}+1)||E\{R_{SP}+1||ACK\_AUTH, K_{KEPCO,SP}\}$. Thus, the SP computes four hash and two symmetric key operations during appliance authentication phase.

Token reissue phase

In token reissue phase, the IC computes four hash and four symmetric key operations totally. To receive $H(R_{IC})||E\{token||R_{IC}||MSG, K_{IC,HS}\}$, one hash and one symmetric key operation is required. Additionally one hash and one symmetric key operation is required to generate MSG_RE, and one hash and one symmetric key operation is required to generate $H(R_{SM})||E\{R_{SM}||MSG\_RE, K_{IC,SM}\}$. To receive $H(R_{SM})||E\{R_{SM}||ACK\_RE, K_{IC,SM}\}$, the IC computes two hash and two symmetric key operations additionally.

The SM has to compute two hash and two symmetric key operations to generate $H(R_{SM'})||E\{R_{SM'}|| MSG\_RE, K_{SM,KEPCO}\}$. One hash and one symmetric key operation are required to reveal MSG_RE from $H(R_{SM})||E\{R_{SM}||MSG\_RE, K_{IC,SM}\}$. Using revealed MSG_RE, the cost for generating $H(R_{SM'})|| E\{R_{SM'}||MSG\_RE, K_{SM,KEPCO}\}$ is one hash and one symmetric key operation. Similarly, the SM has to compute two hash and two symmetric key operations to receive $H(R_{SM'})||E\{R_{SM'}||ACK\_RE, K_{SM,KEPCO}\}$ and send $H(R_{SM})||E\{R_{SM}||ACK\_RE, K_{IC,SM}\}$. Thus, the SM computes four hash and four symmetric key operations during token reissue phase.

When KEPCO receives $H(R_{SM'})||E\{R_{SM'}||MSG\_RE, K_{SM,KEPCO}\}$, it has to compute one hash and one symmetric key operation to reveal $token||H(R'_{IC})||E\{token||R'_{IC}||REQ, K_{IC,SP}\}$. And by using our membership verification scheme, KEPCO finds out a proper SP which receives MSG_RE. During our membership verification scheme, one exponent multiplication and one exponent addition is required. It has to compute one hash and one symmetric key operation to generate $H(R_{SP})||E\{R_{SP}||MSG\_RE, K_{KEPCO,SP}\}$ additionally. Similarly, KEPCO has to compute additional two hash and two symmetric key operations to receive $H(R_{SP}+1)||E\{R_{SP}+1||ACK\_RE, K_{KEPCO,SP}\}$ and send $H(R_{SM'})||E\{R_{SM'}||ACK\_RE , K_{SM,KEPCO}\}$ to the SM. KEPCO computes two hash operations, two symmetric key operations, and one exponent multiplication and one exponent addition during token reissue phase.

The SP has to compute two hash and two symmetric key operations to reveal information included in $H(R_{SP})||E\{R_{SP}||MSG\_RE, K_{KEPCO,SP}\}$. It also requires two exponent multiplications and one exponent addition to generate new token, $token_{new}$. And it has to compute two hash and two symmetric key operations to generate ACK_RE and $H(R_{SP}+1)||E\{R_{SP}+1||ACK\_RE, K_{KEPCO,SP}\}$. Thus the SP computes four hash operations, two symmetric key operations, two exponent multiplications and one exponent addition during token reissue phase.

Token change phase

In token reissue phase, the HS sends $H(R_{IC})||E\{token||R_{IC}||MSG\_CHG, K_{IC,HS}\}$ to an IC. To reveal information in this message, the IC has to compute one hash and one symmetric key operation. The IC replies to the HS with $H(R_{IC})||E\{token_{new}||R_{IC}||MSG\_REG, K_{IC,HS}\}$, thus one hash and one symmetric key operation are required. In final step of token change phase, the IC receives $H(token_{new})||E\{token_{new}||K_{IC,SM}, K_{IC,HS}\}$ from the HS and one hash and one symmetric key operation are required additionally. Totally, three hash operations and three symmetric key operations are required during token change phase for the IC.

The SM receives only $H(token_{new})||E\{token_{new}||K_{IC,SM}, K_{SM,HS}\}$ during token change phase, and the SM computes only one hash and one symmetric key operation during token change phase.

The HS receive new token from the IC by $H(R_{IC})||E\{token_{new}||R_{IC}||MSG\_REG, K_{IC,HS}\}$. To reveal this information, the HS has to compute one hash and one symmetric key operation. And the HS generates new session key between the IC and the SM by using R_{IC} and $token$. During this process one hash operation is required. After generating the new session key, the HS send it to the IC and the SM. $H(token_{new})$ is common for both, thus one hash and two symmetric key operations are required. Thus three hash and three symmetric key operations are required for the HS during token change phase.

Power request phase

In appliance authentication phase, the IC computes one hash and one symmetric key operation to generate $token||H(R'_{IC})||E\{token||R'_{IC}||MSG_REQ, K_{IC,SP}\}$, and one hash and one symmetric key operation is additionally required to generate $H(R_{SM})||E\{R_{SM}||REQ\_POW, K_{IC,SM}\}$. To receive $H(R_{SM})||E\{R_{SM}||ACK\_POW, K_{IC,SM}\}$, the IC computes two hash and two symmetric key operations additionally. Thus, the IC computes four hash and four symmetric key operations during power request phase.

The SM has to compute two hash and two symmetric key operations to generate $H(R_{SM'})||E\{R_{SM'}||$

$REQ\_POW, K_{SM,KEPCO}\}$. One hash and one symmetric key operation is required to reveal REQ_POW from $H(R_{SM})||E\{R_{SM}||REQ\_POW, K_{IC,SM}\}$, and one hash and one symmetric key operation is additionally required to generate $H(R_{SM'})||E\{R_{SM'}||REQ\_POW, K_{SM,KEPCO}\}$ using revealed REQ_POW. Similarly, the SM has to compute two hash and two symmetric key operations to receive $H(R_{SM'})||E\{R_{SM'}|| ACK\_POW, K_{SM,KEPCO}\}$ and send $H(R_{SM})||E\{R_{SM}||ACK\_POW, K_{IC,SM}\}$. Thus, the SM computes four hash and four symmetric key operations during appliance authentication phase.

When KEPCO receives $H(R_{SM'})||E\{R_{SM'}||REQ\_POW, K_{SM,KEPCO}\}$, it has to compute one hash and one symmetric key operation to reveal $token||H(R'_{IC})||E\{token||R'_{IC}||REQ\_POWER, K_{IC,SP}\}$. And by using our membership verification scheme, KEPCO find out a proper SP which receive REQ_POW. During our membership verification scheme, one exponent multiplication and one exponent addition is required. It has to compute one hash and one symmetric key operation to generate $H(R_{SP})||E\{R_{SP}||REQ\_POW$ $, K_{KEPCO,SP}\}$ additionally. Similarly, it has to compute additional two hash and two symmetric key operations to receive $H(R_{SP}+1)||E\{R_{SP}+1||ACK\_POW, K_{KEPCO,SP}\}$ and send $H(R_{SM'})||E\{R_{SM'}$ $||ACK\_POW, K_{SM,KEPCO}\}$ to the SM. KEPCO computes two hash operations, two symmetric key operations, and one exponent multiplication and one exponent addition during appliance authentication phase.

The SP has to compute two hash and two symmetric key operation to reveal information included in $H(R_{SP})||E\{R_{SP}||REQ\_POW, K_{KEPCO,SP}\}$, and two hash and two symmetric key operations to generate ACK_AUTH and $H(R_{SP}+1)||E\{R_{SP}+1||ACK\_POW, K_{KEPCO,SP}\}$. Thus, the SP computes four hash and two symmetric key operations during appliance authentication phase.

Report phase

In report phase, the SM and the HS communicate via symmetric encrypted message. $H(R_{HS})||E\{R_{HS}|| MSG_REPORT||token, K_{SM,HS}\}$ is send by the HS and received by the SM, On the other hand, $H(R_{HS}+1)||E\{R_{HS}+1||MSG\_ACK||POWER_{token}||, K_{SM,HS}\}$ is send by the SM and received by the HS. During this phase, the SM has to compute two hash and two symmetric operations. The HS also has to compute two hash and two symmetric operations.

4.1.3 Communicational Cost

We measure the communicational cost of our protocol by the number of bit of transfered messages. It is described in Table 4.6. If there is no communication in each phase, we notate it as -.

Table 4.6: Communicational Cost(bit)

	App.Reg.	App.Auth.	Tok.Reissue	Tok.Chg.	Pow.Req.	Report
IC → SM	-	1,568	1,568	-	1,568	-
IC → HS	1,824	-	-	800	-	-
SM → HS	-	-	-	-	-	288
SM → KEPCO	-	1,568	1,568	-	1,568	-
KEPCO → SP	-	1,568	1,568	-	1,568	-
SP → KEPCO	-	544	1,056	-	1,056	-
KEPCO → SM	-	544	1,056	-	1,056	-
HS → SM	928	-	-	800	-	1,824
HS → IC	928	-	800	1,600	-	-
SM → IC	-	544	1,056	-	1,056	-

Appliance registration phase

The IC sends $H(R_{IC})||E\{token||R_{IC}||MSG_REG, K_{IC,HS}\}$ to the HS. The length of $H(R_{IC})|| E\{token||R_{IC}||MSG_REG, K_{IC,HS}\}$ is $160 + E\{512 + 64 + 8 + 1024\} = 160 + 1,664 = 1,824(bit)$. So, the communicational cost for the IC is 1,824 bit.

The HS sends $H(token)||E\{token||K_{IC,SM}||R_{SM}, K_{SM,HS}\}$ and $H(token)||E\{token||K_{IC,SM}||R_{SM}, K_{IC,HS}\}$. Both messages have same length, such as $160 + E\{512 + 128 + 64\} = 160 + 768 = 928(bit)$. Thus, the communicational cost for the HS is 928 bit.

Appliance authentication phase

The IC sends $H(R_{SM})||E\{R_{SM}||MSG\_AUTH, K_{IC,SM}\}$ to the SM. The length of MSG_AUTH is $512 + 160 + E\{512 + 64 + 8\} = 512 + 160 + 640 = 1,312(bit)$. Thus, the length of the message which IC sends is $160 + E\{64 + 1312\} = 160 + 1,408 = 1,568(bit)$. So, the communicational cost for the IC is 1568 bit.

The SM sends $H(R_{SM'})||E\{R_{SM'}||MSG\_AUTH, K_{SM,KEPCO}\}$ and $H(R_{SM})||E\{R_{SM}||ACK\_AUTH, K_{IC,SM}\}$. The length of ACK_AUTH is $160 + E\{64 + 8\} = 160 + 128 = 288(bit)$. Thus, the length of

$H(R_{SM'})||E\{R_{SM'}||MSG\_AUTH, K_{SM,KEPCO}\}$ is $160 + E\{64 + 1312\} = 160 + 1,408 = 1,568(bit)$ and the length of $H(R_{SM})||E\{R_{SM}||ACK\_AUTH, K_{IC,SM}\}$ is $160 + E\{64 + 288\} = 160 + 384 = 544(bit)$. Thus, the communicational cost for the SM is $1,568 + 544 = 2,112(bit)$, 2,112 bit.

Similarly, KEPCO sends $H(R_{SP})||E\{R_{SP}||MSG\_AUTH, K_{KEPCO,SP}\}$ and $H(R_{SM'})||E\{R_{SM'}$ $||ACK\_AUTH, K_{SM,KEPCO}\}$. The length of each message is same as that of the SM. So, the communicational cost for the KEPCO is 2,112 bit.

Lastly, the SP sends $H(R_{SP} + 1)||E\{R_{SP} + 1||ACK\_AUTH, K_{KEPCO,SP}\}$ to KEPCO. The length of this message is $160 + E\{64 + 288\} = 160 + 384 = 544(bit)$. Thus, the communicational cost for the SP is 544 bit.

Token reissue phase

The HS sends $H(R_{IC})||E\{token||R_{IC}||MSG, K_{IC,HS}\}$ to the IC during first stage of token reissue phase. The length of MSG_RE is $512 + 160 + E\{512 + 64 + 8\} = 512 + 160 + 640 = 1,312(bit)$. So, the message requires $160 + E\{512 + 64 + 8\} = 160 + 640 = 800(bit)$ communicational cost for the HS.

The IC sends $H(R_{SM})||E\{R_{SM}||MSG\_RE, K_{IC,SM}\}$ to the SM. The length of this message is $160 + E\{64 + 1,312\} = 160 + 1,408 = 1,568(bit)$. So, the communicational cost for the IC is 1,568 bit.

The SM sends $H(R_{SM'})||E\{R_{SM'}||MSG\_RE, K_{SM,KEPCO}\}$ and $H(R_{SM})||E\{R_{SM}||ACK\_RE, K_{IC,SM}\}$. The length of ACK_RE is $160 + E\{64 + 512 + 8\} = 160 + 640 = 800(bit)$. Thus, the length of $H(R_{SM'})||E\{R_{SM'}||MSG\_RE, K_{SM,KEPCO}\}$ is $160 + E\{64 + 1,312\} = 160 + 1,408 = 1,568(bit)$ and the length of $H(R_{SM})||E\{R_{SM}||ACK\_RE, K_{IC,SM}\}$ is $160 + E\{64 + 800\} = 160 + 896 = 1,056(bit)$. Thus, the communicational cost for the SM is $1,568 + 1,056 = 2,624(bit)$, 2,624 bit.

Similarly, KEPCO sends $H(R_{SP})||E\{R_{SP}||MSG\_RE, K_{KEPCO,SP}\}$ and $H(R_{SM'})||E\{R_{SM'}||ACK\_RE$ $, K_{SM,KEPCO}\}$. The length of each message is same as that of the SM. So, the communicational cost for the KEPCO is 2,624 bit.

Lastly, the SP sends $H(R_{SP} + 1)||E\{R_{SP} + 1||ACK\_RE, K_{KEPCO,SP}\}$ to KEPCO. The length of this message is $160 + E\{64 + 800\} = 160 + 896 = 1,056(bit)$. Thus, the communicational cost for the SP is 1,056 bit.

Token change phase

In token change phase, the HS sends $H(R_{IC})||E\{token||R_{IC}||MSG\_CHG, K_{IC,HS}\}$ to the IC. The length of this message is $160 + E\{512 + 64 + 8\} = 160 + 640 = 800(bit)$. And the HS sends $H(token_{new})||E\{token_{new}||K_{IC,SM}, K_{SM,HS}\}$ to the SM and sends $H(token_{new})||E\{token_{new}||K_{IC,SM}, K_{IC,HS}\}$ to the IC. These two messages have same length, such as $160+E\{512+128\} = 160+640 = 800$. Thus the communicational cost of the HS is $800 + 800 \times 2 = 2,400(bit)$, 2,400 bit.

On the other hand, the IC sends $H(R_{IC})||E\{token_{new}||R_{IC}||MSG\_REG, K_{IC,HS}\}$ to the HS. The length of this message is $160 + E\{512 + 64 + 8\} = 160 + 640 = 800(bit)$. So the communicational cost of the IC is 800 bit.

Power request phase

The IC sends $H(R_{SM})||E\{R_{SM}||REQ\_POW, K_{IC,SM}\}$ to the SM. The length of REQ_POW is $512 + 160 + E\{512 + 64 + 8\} = 512 + 160 + 640 = 1,312(bit)$. Thus, the length of the message is $160 + E\{64 + 1,312\} = 160 + 1,408 = 1,568(bit)$. So, the communicational cost for the IC is 1,568 bit.

The SM sends $H(R_{SM'})||E\{R_{SM'}||REQ\_POW, K_{SM,KEPCO}\}$ and $H(R_{SM})||E\{R_{SM}||ACK\_POW, K_{IC,SM}\}$. The length of ACK_POW is $160+E\{64+512+8\} = 160+640 = 800(bit)$. Thus, the length of $H(R_{SM'})||E\{R_{SM'}||REQ\_POW, K_{SM,KEPCO}\}$ is $160 + E\{64 + 1,312\} = 160 + 1,408 = 1,568(bit)$ and the length of $H(R_{SM})||E\{R_{SM}||ACK\_POW, K_{IC,SM}\}$ is $160 + E\{64 + 800\} = 160 + 896 = 1,056(bit)$. Thus, the communicational cost for the SM is $1,568 + 1,056 = 2,624(bit)$, 2,624 bit.

Similarly, KEPCO sends $H(R_{SP})||E\{R_{SP}||REQ\_POW, K_{KEPCO,SP}\}$ and $H(R_{SM'})||E\{R_{SM'}|| ACK\_POW, K_{SM,KEPCO}\}$. The length of each message is same as that of the SM. So, the communicational cost for the KEPCO is 2,624 bit.

Lastly, the SP sends $H(R_{SP} + 1)||E\{R_{SP} + 1||ACK\_POW, K_{KEPCO,SP}\}$ to KEPCO. The length of this message is $160 + E\{64 + 800\} = 160 + 896 = 1056(bit)$. Thus, the communicational cost for the SP is 1,056 bit.

Report phase

In report phase, the HS sends $H(R_{HS})||E\{R_{HS}||MSG_REPORT||token, K_{SM,HS}\}$ to the SM. The length of this message is $160+E\{64+8+1024+512\} = 160+1,664 = 1,824(bit)$. So, the communicational cost for the HS is 1,824 bit.

On the other hand, the SM sends $H(R_{HS}+1)||E\{R_{HS}+1||MSG_ACK||POWER_{token}, K_{SM,HS}\}$ to the HS. The length of this message is $160 + E\{64+8+32\} = 160+128 = 288(bit)$. Thus the communicational cost for the SM is 288 bit.

4.2 Security Analysis

4.2.1 Mutual authentication

Entity which is participated in communication has shared a key for each other. In detail, the shared keys are $K_{IC,SM}$, $K_{IC,HS}$, $K_{IC,SP}$, $K_{SM,HS}$, $K_{SM,KEPCO}$, and $K_{KEPCO,SP}$. By using shared key, entities which are participated in communication can authenticate mutually.

4.2.2 Confidentiality & Integrity

All messages are encrypted by a fresh session key. Only the entity (*i.e.,* smart appliance and smart meter) having the session key can identify the contents of encrypted message. Thus, we can provide confidentiality. The integrity of message is also confirmed by comparing nonces concatenated in front of message and nonces which encrypted in message.

4.2.3 Anonymity

Although the outsider including an adversary can easily eavesdrop the communications over HAN, he cannot reveal the content of message because the message was encrypted.

On the other hand, the SM cannot distinguish the type of an appliance. The SM cannot reveal the power consumption for each device since the SM does not have any information about a relationship between the token and the appliances. However, as the adversary infers to the power consumption of each appliance from the power consumption of each token, our protocol employs periodic update of the token owned by each device.

As a result, we believe that our protocol can support anonymity of an end-user from the insiders and outsiders.

4.2.4 Resiliency against compromising smart meter

Although the adversary cannot access the home server of the target end-user, he may compromise the smart meter in HAN. Through compromising the smart meter, the adversary can obtain useful information.

However, in our protocol the adversary cannot identify the type of appliance used in HAN through the stored information in SM because the token $E[-r, PK_{BGN}, G]$, which is used to authenticate the appliances, only indicates that the appliance is owned by an SP. The relationship between the token and target appliance is only known to the service provider. Moreover, the adversary cannot identify the target appliance of the token in polynomial time since the BGN encryption requires the $\tilde{O}(\sqrt{|T|})$ time for decryption although the adversary has the private key, $SK_{BGN} = q_1$ [6]. From these observations, we provide resiliency against compromising the smart meter.

The end user is may want to compromise his smart meter. Even the end user compromises his smart meter, he cannot gain economical advantages such as electricity tariff discount. Our protocol confirms whether an appliance is the target of electricity tariff discount by mutual check by IC and SP, and this mutual check depends on the nonce and session key which is hardcoded when the IC is manufactured. Thus even the end user compromises his smart meter, this try cannot pass mutual check between IC and SP. So, we also provide resiliency against compromising the smart meter by the end user.

Chapter 5. Conclusion

In this paper, we propose an efficient privacy-preserving authentication for HAN over the SG system. Our protocol satisfies the security requirements such as mutual authentication, confidentiality, message integrity, anonymous communication, and resiliency against compromising SM(smart meter). We analyze the security of our protocol, in detail for the practical application.

The scheme which proposed by Georgios *et al.* [12] hides the usage pattern of electricity by adopting rechargeable battery. But this scheme does not consider mutual authentication and protect the private information of user, such as, social security number. On the other hand, the scheme which proposed by Efthymiou *et al.* [13] concerns protecting the private information of user, but it does not consider hiding the usage pattern of electricity and preventing compromising SM.

The protocol which proposed by Rial *et al.* [14] satisfies the security requirements, such as, mutual authentication, confidentiality, integrity, anonymity, and resiliency against compromising SM, whici required in our protocol. This protocol requires 10,586 KB to transmit the proof associated with 1,000 meter readings with 2,048 bit RSA modulus, and 6,586 KB to transmit the proof associated with 1,000 meter readings with 1,024 bit RSA modulus. On the other hand, our protocol requires about 2,624 KB for the SM with 1,000 meter readings(Power Request). Their protocol requires lots of bits to communicate because it using public key signature to authenticate each entities. Our protocol is based on the symmetric key encryption and hash, thus it requires about few KB to communicate each entity. On the other hand, our protocol occurs some burden for managing symmetric keys. But, the IC and the SM, which have lower computational power, have to manage only 2 or 3 symmetric keys. KEPCO or SP, which has to manage thousands of keys, has strong computational power thus key management is not heavy for KEPCO and SP. Moreover our protocol use membership verification scheme, thus the time which KEPCO finding appropriate SP is not $O(n)$, but $O(1)$, when n is number of registered IC.

Our protocol fulfills security requirements, such as, mutual authentication, confidentiality, integrity and anonymity. Moreover our protocol also satisfies resiliency against compromising SM. Mutual authentication is achieved by applying symmetric key encryption between each communicating entity. We can achieve confidentiality and integrity by adding hash value of the secret which only the communicating entities know. To keep anonymity, we using the token of our membership verification instead of identity of IC. Thus we can hide the type of appliance and the fabricant of the IC. Our protocol satisfies resiliency against compromising SM by mutual authentication between IC and SP. Moreover even the adversary compromises SM, he cannot add the appliance into the existed membership. At the same time, our protocol offers lightweightness. Lightweightness is very important for protocols which perform on HAN, because the core entities for HAN, such as the SM, have only limited computational power. To satisfy lightweightness, our protocol is based on the symmetric key operation and hashing operation. Moreover our membership verification reduces the cost for find out appropriate SP signficantly. By those practice, our protocol can achieve lightweightness.

Summary

A Study on Privacy-preserving Authentication Scheme in Home Area Network under Smart Grid system

스마트 그리드는 기존의 전력망에 디지털 통신 기술을 활용하여 전력망 구성요소 및 참여자들 간에 양방향 통신이 가능케 하는 기술이다. 양방향 통신을 통해 기존의 전력망에서는 불가능했던 다양한 기능 등이 가능해졌는데, 전력망 부하에 따른 차등 요금제, 부하 분산을 통한 전력망의 안정성 향상, 가전기기의 원격제어, 정책적인 목적에서의 전력 요금제 도입 등이 그 예이다. 한편, 양방향 통신을 통해 기존에는 제공되지 않던 정보가 통신망에 노출됨으로써 개인 정보의 침해가 우려되고 있으며, 경제적인 이득을 노린 부정한 사용의 가능성 또한 존재한다. 이에 따라 스마트 그리드가 정착되기 위해서는 공격자의 악의적인 공격을 막고 사용자의 개인 정보를 보호하며, 부정한 사용을 방지할 수 있는 기술에 대한 연구가 선행되어야 한다. 이 점은 모든 사람들이 공감하며 최근 많은 연구들이 진행되고 있다.

본 학위 논문에서는 스마트 그리드 시스템의 댁내망에서의 새로운 인증 기법을 제안한다. 우리가 제안한 기법은 사용자에게 개별 기기의 전력 사용량 측정, 효율성을 위한 선행적인 전력 요청, 전기 자동차 등의 정책적인 혜택이 있는 가전기기에 대한 지원과 같은 다양한 기능을 제공한다. 동시에 인증, 신뢰성 및 무결성, 익명성을 동시에 만족하며, 공급자의 측면에서 우려되는 사용자에 의한 스마트 미터의 조작을 통한 부당한 요금 할인 또한 방지할 수 있다. 또한 수사 등의 목적으로 필요시에는 사용자와 충전 장소, 시간 등의 정보를 복원할 수 있는 추적가능성 또한 만족한다. 익명성과 추적가능성은 서로 상반되는 속성이다. 우리는 상반되는 두 속성을 동시에 만족시키기 위해 공신력 있는 기관에 정보를 분산하는 방식을 택하였다. 각각이 소유하고 있는 정보만으로는 사용자의 위치정보를 추적할 수 없으나, 특수한 경우에 한해 양측이 소유하고 있는 정보를 통합함으로써 사용자의 위치정보를 복원할 수 있다.

우리가 제안한 기법은 기존 기법들과 비교하여 경량성에서도 효율적일 뿐 아니라, 기존 기법에서 고려하지 않은 누진세 면제와 같은 정책적인 측면에서 제공되는 요금 할인 혜택을 얻기 위한 사용자에 의한 스마트 미터 조작에 대한 대비 또한 이루어지고 있다. 동시에 공격자에 의한 가전기기 별 전력 사용량의 역추적과 같은 공격을 특별한 물리적인 장치(축전지)의 추가 없이 방지할 수 있으며, 이러한 방지에 멤버쉽 인증을 도입함으로써, 빈번한 통신이 발생하는 큰 규모의 네트워크에서 인증 및 키 관리 면에서 효율적으로 동작하도록 해준다.

References

[1] G.A. McNaughton, R. Saint, "Enterprise integration implications for home-area network technologies," *Innovative Smart Grid Technologies (ISGT), 2010, pp. 1-5.*

[2] H. Khurana, M. Hadley, Ning Lu, and D.A. Frincke, "Smart-Grid Security Issues," *Security & Privacy, IEEE, vol. 8, pp. 81-85, 2010.*

[3] NIST, *Guidelines for Smart Grid Cyber Security, Aug, 2010*, vol 1-3.

[4] P. McDaniel, and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *Security & Privacy, IEEE, 2009*, pp. 75-77

[5] F.M. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," *Power and Energy Society General Meeting, 2008.*

[6] D. Boneh, E.-J. Goh and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," *Theory of Cryptography (TCC '05), LNCS 3378, Feb. 2005*, pp. 325-341

[7] J. M. Pollard, "Kangaroos, Monopoly and Discrete Logarithms," *Journal of cryptology, 2000*, vol 13, Number 4, pp. 437-447

[8] S. S. Yau and Y. Yin, "Controlled Privacy-preserving Keyword Search," *Proc. of ACM Symposium on Information, Computer & Communications Security (ASIACCS '08), Mar. 2008*, pp. 321-324.

[9] M. J. Freedman, K. Nissim and B. Pinkas, "Efficient Private Matching and Set Intersection," *Advanced in Cryptography - EUROCRYPT '04, LNCS 3027, May 2004*, pp. 1-19.

[10] L. Kissner and D. X. Song, "Privacy-preserving Set Operations," *Advances in Cryptology - CRYPTO '05, LNCS 3621, Aug. 2005*, pp. 241-257.

[11] Jangseong Kim, Joonsang Baek, Kwangjo Kim and Jianying Zhou, "A Privacy-Preserving Secure Service Discovery Protocol for Ubiquitous Computing Environments," *Proc. of EuroPKI 2010, Sep. 23-24, 2010, Athens, Greece.*

[12] G. Kalogridis, C. Efthymious, S.Z. Denic, T.A. Lewis and R. Cepeda, “Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures,” *Smart Grid Communications (SmartGridComm), 2010, pp. 232 - 237.*

[13] C. Efthymiou and G. Kalogridis, “Smart Grid Privacy via Anonymization of Smart Metering,” *Smart Grid Communications (SmartGridComm), 2010, pp. 238 - 243.*

[14] A. Rial and G. Danezis, “Privacy-Preserving Smart Metering,” *research.microsoft.com, 2010.*

[15] G. W. Hart, “Nonintrusive appliance load monitoring,” *Proceedings of the IEEE, December 1992, pp. 1870-1891.*

[16] C. Laughman, K. Lee, R. Cox, S. Shaw, S. Leeb, L. Norford and P. Armstrong, “Power signature analysis,” *Power and Energy Magazine, IEEE, vol. 1, no. 2, pp. 56-63, 2003.*

Acknowledgement

본 논문을 완성하는데 정말 많은 분들의 도움이 있었습니다. 도움을 주신 모든 분들께 감사드립니다. 김광조 교수님께서는 틈틈히 연구 상황을 확인해 주셔서 체계적인 연구방향을 세울 수 있었습니다. 그리고 암호와 정보보호 연구실에서 함께 연구실 생활을 한 선후배님 (현록이형, 규석이형, 진이형, 장성이형, Duc, Divyan, 준현이, Made, 이재) 들에게 연구실 생활 및 연구 등 많은 부분에서 격려 및 도움을 받았습니다. 바쁘신 와중에 학위논문심사를 위해 참석하셔서 진심어린 조언을 주신 박진아 교수님과 이기혁 교수님께도 감사드립니다. 오늘의 제가 있게 해주신 우리 가족, 부모님께 감사드립니다. 마지막으로, 제가 태어난 대한민국에 감사의 말을 전합니다.

이 력 서

이　　　름 : 정 도 영

생 년 월 일 : 1986년 9월 20일

주　　　소 : 대전광역시 유성구 신성동 럭키하나아파트 102동 402호

E-mail 주 소 : wordspqr@kaist.ac.kr

학 력

2002. 3. – 2005. 2.　대덕고등학교

2005. 2. – 2010. 2.　카이스트 전산학과 (B.S.)

2010. 2. – 2012. 2.　카이스트 전산학과 (M.S.)

경 력

2011. 7. – 2011. 8.　LG 유플러스 Device개발실 HT단말개발팀 인턴연구원

연 구 업 적

1. **Doyoung Chung**, Made Harta Dwijaksara, Yi Jae Park, Jangseong Kim and Kwangjo Kim, "An Efficient and Privacy Preserving Authentication Protocol for HAN", 2011 Symposium on Cryptography and Information Security (SCIS 2011), Jan. 25-28, 2011, Kokura, Japan.

2. Yi Jae Park, **Doyoung Chung**, Made Harta Dwijaksara, Jangseong Kim and Kwangjo Kim, "An Enhanced Security Policy Framework for Android", 2011 Symposium on Cryptography and Information Security (SCIS 2011), Jan. 25-28, 2011, Kokura, Japan.

3. Made Harta Dwijaksara, **Doyoung Chung**, Yi Jae Park, Jangseong Kim and Kwangjo Kim, "Secure, Fast Rebuilding and Energy Efficient Routing Protocol for Mission Critical Application

over Wireless Sensor Networks”, 2011 Symposium on Cryptography and Information Security (SCIS 2011), Jan. 25-28, 2011, Kokura, Japan.

4. **정도영**, 김장성, Made Harta Dwijaksara, 박이재, 김광조, ”스마트그리드에서 전기자동차 충전을 위한 안전한 인증 및 과금 결재 프로토콜”, CISC-S‘11 Proceedings, pp.221-226, 2011.6.24. 충남대학교 (우수논문) [2010]

5. Yi Jae Park, **Doyoung Chung**, Made Harta Dwijaksara, Jangseong Kim and Kwangjo Kim, “An Enhanced Security Policy Framework for Android”, Program of Triangle Symposium on Advanced ICT 2011 (TriSAI 2011), Aug. 25-26, 2011, KAIST, Korea.