Privacy Enhancement and Secure Data Transmission Mechanism for Smart Grid System

Shi Li, Kyung Choi, Inshil Doh, Kijoon Chae
Dept. of Computer Science and Engineering, Ewha Womans University
e-mail : lishi1116@ewhain.net, cbk0907@ewhain.net, isdoh@ewhain.net, kjchae@ewha.ac.kr

Abstract

With the growth of Smart Grid technologies, security and privacy will become the most important issues and more attention should be paid. There are some existing solutions about anonymization of smart meters, however, they still have some potential threats. In this paper, we describe an enhanced method to protect the privacy of consumer data. When metering data are required by a utility or the electrical energy distribution center for operational reasons, data are delivered not with the real IDs but with temporary IDs. In addition, these temporary IDs are changed randomly to prevent the attackers from analyzing the energy usage patterns. We also describe secure data transmission method for securing data delivered. In this way, we can enhance the privacy of Smart Grid System with low overhead.

1. INTRODUCTION

Modernization efforts are underway to make the current electrical grid "smarter." The infrastructure that supports the future Smart Grid will be capable of informing consumers of their day-to-day energy use, even at the appliance level. The smart grid [1] uses intelligent transmission and distribution networks to deliver electricity. This approach aims to improve the electric system's reliability, security, and efficiency through two-way communication of consumption data and dynamic optimization of electric-system operations, maintenance, and planning. Smart Metering is a key component of the future vision of smart grid[2].

Smart meters enable two-way communication between the meter and the central system. Unlike home energy monitors, smart meters can gather data for remote reporting. Smart meter as an advance detail electricity information collector, can include the customer's privacy. The customer habits and behaviors may be exposed. It might also be possible to discover what types of appliances and devices are present by compromising either the customer's home area network or the AMR network. How can we prevent the utility from knowing the privacy, without affecting the normal management and control? In this paper, we propose a privacy enhancement mechanism by screening the real IDs from the utilities or the energy center by using temporal IDs, and we also propose secure transmission mechanism.

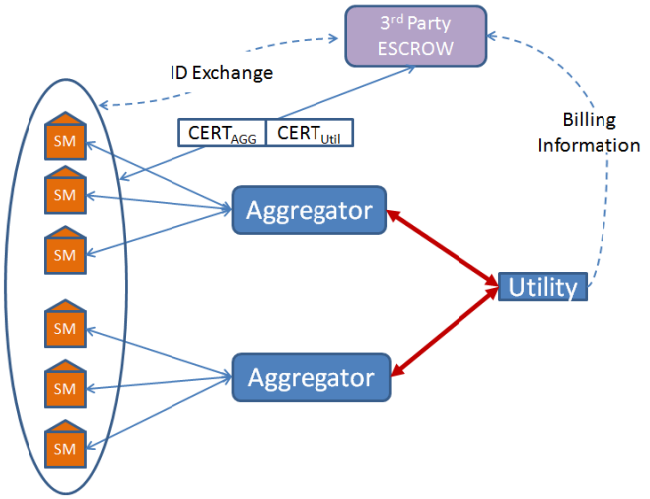
This paper is organized as follows: Section 2 briefly discusses the background of metering privacy issues, and section 3 discusses the smart grid privacy enhancement mechanism including the process of screening identities and securing transmission. The conclusions are drawn in Section 4.

2. RELATED WORK

The method named anonymization of Smart Metering Data proposed by Costas Efthymiou and Georgios Kalogridis [3] addresses the privacy problem by anonymous smart metering data so that information gleaned from it cannot easily be associated with an identified person. Metering data are divided into 'High-frequency (anonymous)' metering data and 'Low-frequency (attributable)' metering data. The 'High-frequency' metering data may expose private information, so it should be anonymized. The main structural difference to a smart meter introduced is that there are two separate IDs embedded in the smart meter, rather than a single ID as is the case with standard smart meters. To achieve the purpose of privacy, a 3rd party escrow mechanism for authenticated anonymous meter readings is provided, which are difficult to associate with a particular smart meter or customer. For a utility can be sure that messages being received from a specific HFID can be authenticated, the CDP (Client Data Profile) and ADP (Anonymous Data Profile) are provided. CDP will be attached to each low-frequency metering message from the smart meter to the utility, which includes the certificate information of attributable smart meter, aggregator, the utility and so on. The problem of this mechanism is that in LFID case, aggregators and utility can get the certificate information of the data and the real IDs can be revealed. In addition, even if they cannot get the IDs, with a lot of data accumulated, they can guess the energy usage patterns. In this paper, we try to address this privacy problem.

3. PROPOSED SMART GRID PRIVACY PROTECTION MECHANISM

There are some potential privacy problems in smart grid systems. One of the problems is that the utility may manage the smart meter distributed in a specific area. Over a long period of time, the utility can speculate the privacy information based on the users or smart meters managed and can analyze the data received. Another problem is the security protection during communication, i.e. an attacker could locate near a house and intercept the message sent from that house (he may know the data and the data source). To solve the first problem, we propose a mechanism which frequently alters the IDs to protect the privacy of consumer. For the security of data transmission, we also propose series of processes for secure data transmission. [Fig.1] shows the system overview of our proposal.



[Fig. 1] System overview of Smart Grid system for privacy protection

3.1 ASSUMPTION

Our smart grid system includes four parts: Smart Meter (SM), 3rd party ESCROW, Aggregator (AGG), Utility (U). The 3rd party escrow can provide the certificates to the temporary ID. We also assume that the aggregator and utility know and recognize the certificates of the smart meter, $CERT_{AGG}$ and $CERT_{Util}$, respectively.

An adequate trust relationship is present among the 3rd party escrow service providers, utility companies and their customers. More specifically, escrow service providers should be trusted not to provide customer information to utility companies, and should also be trusted to securely provide anonymization credentials that cannot be repudiated. Only 3rd party Escrow knows the relationship between real IDs and temporary IDs of smart meters. Between Smart Meter and 3rd party ESCROW share symmetric keys, and Aggregator and Utility use public and private keys.

3.2 IDENTITY ALTERATION MECHANISM

Initially, we distribute a temporary ID to each smart meter. Smart meter can use this temporary ID to identify itself when sending data to utility. The utility can manage the information using this ID without knowing the true identity of the smart meter. This can protect the privacy of the customer.

Each smart meter shares symmetric key with the 3rd party escrow. A smart meter generates a random ID and sends it as a request to the 3rd party periodically after encrypting it with symmetric keys. The 3rd party checks the table (see <Table1>) which includes the information of the smart meters to verify this new ID. If verified, the new ID will be inserted into the table, and the verified certificate is sent to the smart meter as a response. The smart meter uses the new verified ID to identify itself after receiving the positive response from the 3rd party. Conversely, if unverified, the new ID will be ignored and the ID used in the previous period will be recorded again in the next period. Then the negative response will be sent from the 3rd party to the smart meter for it to use the previous ID for another session. All of these processes are encrypted by the symmetric key, K_{sym}, between the smart meter and the 3rd party.

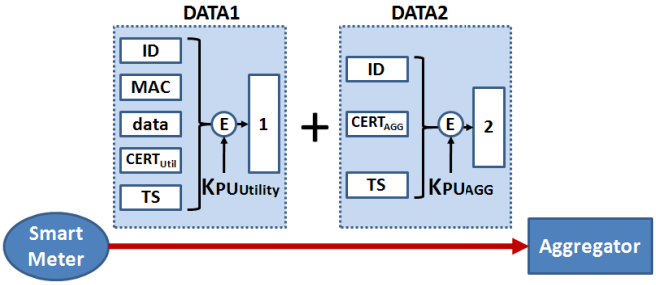
<Table 1> Table in the 3rd Party Escrow

Smart Meter	ID	Time	Certificate
SM1	Id 1-1	2011.03.01	CERT 1
	Id 1-1	2011.04.01	CERT 1
	Id 1-3	2011.05.01	CERT 3

SM→3rd party : E_{Ksym}(New ID)
3rd party→SM : E_{Ksym}(Response)

3.3 SECURE TRANSMISSION PROCESS

To protect the security of the metering data and to avoid potential privacy revealed, we use MAC(Message Authentication Code)[4]. Smart meters encrypt the data, MAC of data, temporary id (ID), timestamp, and the certificate ($CERT_{Util}$) received from 3rd party with the public key of utility to generate DATA1. Smart meters also encrypt the $CERT_{AGG}$, ID and timestamp with aggregator's public key to generate DATA2. Then DATA1 and DATA2 are attached together and sent to aggregator. The process can be seen in [Fig. 2].

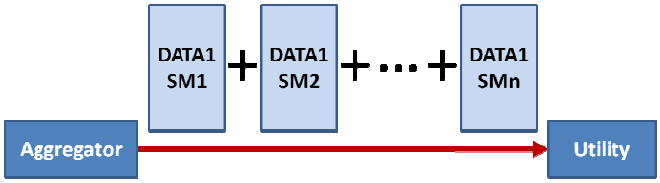


[Fig. 2] Data transmission from Smart Meter to Aggregator

SM→AGG : DATA1||DATA2

DATA1 : $E_{KPU_{Util}}$ (ID||MAC||data||$CERT_{Util}$||timestamp)
DATA2 : $E_{KPU_{AGG}}$ (ID||$CERT_{AGG}$||timestamp)

After receiving the data (DATA1||DATA2) from smart meter, the aggregator decrypts the DATA2 with its private key and checks the $CERT_{AGG}$. If certificated, it sends all the DATA1 aggregated from smart meters to utility. The process can be seen in [Fig. 3].



[Fig. 3] Data transmission from Aggregator to Utility

AGG→Utility : $DATA1_{SM1}$|| ... ... ||$DATA1_{SMn}$

Utility decrypts all DATA1s with its own private key. If further management is necessary, the utility could send management messages, smart meter ID and timestamp to the

3rd party escrow, and this message could be forwarded to smart meter using the temporary ID during the session.

4. CONCLUSION

Privacy concerns are very important for the future deployment of smart meters and smart grid networks, as the amount of data collected from future smart meters will be huge, and privacy will be one of the major issues. In this paper, we address the smart metering privacy issue by screening the IDs of the smart meters. This can provide enhanced protection for privacy. We also describe secure transmission mechanism, and this can further protect the security and privacy of users. For our future research, we will simulate our proposed mechanism and analyze the performance.

ACKNOWLEDGEMENT

This work was supported by Mid-career Researcher Program through NRF grant funded by the MEST(No. 2009-0083985).

REFERENCES

[1] H. Khurana, M. Hadley, Ning Lu, D. A. Frincke, "Smart-Grid Security Issues," Security & Privacy, IEEE, pp.81–85, 2010.

[2] A. H. Rosenfeld, D. A. Bulleit, R. A. Peddie, "Smart Meters and Spot Pricing: Experiments and Potential," IEEE Technology and Society Magazine, vol.5, no.1, pp.23-28, March 1986.

[3] C. Efthymiou, G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," 1st International Conference on Smart Grid Communications (SmartGridComm), IEEE, pp.238-243, 2010.

[4] William Stallings, "Network Security Essentials-Applications and Standards (4th Edition)," PEARSON, pp.77-80, 2011.