Selling Power Back to the Grid in a Secure and Privacy-Preserving Manner

Tat Wing Chim[1], Siu Ming Yiu[1], Lucas Chi Kwong Hui[1], Victor On Kwok Li[2], Tin Wing Mui[1], Yu Hin Tsang[1], Chun Kin Kwok[1], and Kwun Yin Yu[1]

[1] Department of Computer Science
[2] Department of Electrical and Electronic Engineering
The University of Hong Kong, Pokfulam Road, Hong Kong
{twchim,smyiu,hui}@cs.hku.hk, vli@eee.hku.hk,
{twmui,yhtsang,ckkwok,kyyu2}@cs.hku.hk

Abstract. Smart grid facilitates a customer to sell unused or self-generated power back to the grid. This not only helps the power operator to reduce power generation, but also brings customers a means of getting revenue. However, the process of power selling induces two security problems, namely authentication and privacy-preservation. Like other messages, a customer's request messages for power selling should be properly authenticated to avoid various attacks. At the same time, the customer's privacy such as daily electricity usage pattern should be properly protected. In this paper, we propose a secure and privacy-preserving protocol to make this possible. Basically, authentication is done by means of anonymous credentials. Even in the reconciliation phase, the power operator only knows how much power a customer has uploaded to the grid but cannot know when the customer has done so. We evaluate our scheme to show that it is effective.

Keywords: smart grid, power selling, authentication, privacy-preservation, anonymous credential, blind signature.

1 Introduction

Smart grid is the next generation power grid. It integrates information and communication technology with power generation and distribution technologies. Its basic function is to facilitate the power operator to adjust the amount of power generated based on customers' demands. It ensures that customers' demands are satisfied while excess electricity generation can be avoided. This in turn can help protect the environment by reducing air pollutants emitted from the power generation process (especially those by fossil-fuel generators).

In the old days, power transmission is always one-way (i.e. from power grid to customers). The other way (i.e. from customers back to power grid) is impossible. However, the introduction of smart grid changes this picture. Selling power back to the power grid becomes common in U.S. and European countries [1]. The mechanism is in fact beneficial to both the power operator and the customers. The power operator

T.W. Chim and T.H. Yuen (Eds.): ICICS 2012, LNCS 7618, pp. 445–452, 2012.

can "recycle" customers' unused or self-generated power so that it can reduce the amount of power generated and thus lower the expenses. The customers can obtain revenue by selling power. Suppose a customer owns an electric vehicle. Due to differential pricing of electricity, the customer can charge up the battery in his electric vehicle during the low tariff hours, and sell the electricity back to the grid during the high tariff hours. In some countries, to encourage citizens to build renewable generation facilities such as wind mills and solar panels, the government dictates that the utility company has to buy electricity from the customers at a given tariff.

Basically, when a customer wants to sell power back to the grid, he/she has to first make a request with the amount of power to be uploaded to the control center. The control center then authenticates and approves the request. After that, the customer starts uploading power to the grid. As the power transmission system and the communications system are independent of each other, one may ask how the control center can ensure that the customer really upload the amount of power agreed in the request. To facilitate such checking, the smart meter in the customer's home has to be upgraded so that it can measure bi-directional power transmission (i.e. from grid to customer and from customer back to grid). The mechanism of power uploading and how a smart meter can measure bi-directional power transmission are out of the scope of this paper.

This paper focuses on the security and privacy issues in the communications involved in power selling between the control center and smart meters. Two security problems, namely authentication and privacy-preservation are addressed. Like other messages, a customer's request messages for power uploading should be properly authenticated. Otherwise, an attacker can generate numerous fake request messages so as to affect the power operator's decision about power generation. At the same time, the customer's privacy such as daily electricity usage pattern should be properly protected. If a criminal obtains this information, the family is susceptible to being burglarized. Thus we propose a secure and privacy-preserving protocol to resolve both problems. Basically, authentication is done by means of anonymous credentials (analogous to tickets). A customer first generates a set of credentials and blinding factors. The customer "blinds" the credentials and then requests the control center to sign them using the control center's private key. Interested readers may refer to our previous work [13] for details about the blind signature technique. When the customer wants to sell power to the grid, he/she will send an appropriate number of credentials (to represent the amount of power to upload) to the control center anonymously. In the reconciliation phase, the control center computes the number of used credentials to estimate how much power the customer has agreed to upload to the grid (but cannot know when the customer has done so), and then compares this value with the smart meter measurement. If the values are comparable, payment will be made to the customer accordingly. We evaluate our scheme to show that it is effective.

The rest of the paper is organized as follows: related work is summarized in Section 2. The system model and the security requirements are described in Section 3. Our scheme is presented in Section 4. The analysis of our scheme is given in Section 5. Finally, Section 6 concludes the paper.

2 Related Work

The smart grid project was started by the European Union in 2003 [6]. At about the same time, the U.S. Electric Power Research Institute started the IntelliGrid Project [7] and the US DOE also initiated the Grid 2030 project [8]. In early 2010, NIST released a report [5] which describes the potential components and cyber security issues of the smart grid system. As such, smart grid research and development is an important engineering trend in most developed and developing countries.

Two recent works [9] and [10] elaborate the importance of a smart grid especially with the consideration of renewable energy resources. They propose a communication-oriented smart grid framework. New requirements of the communication architecture and possible security problems of the smart grid system are also identified.

Some major security problems have been pointed out and studied in [3] and [4]. On the communication between the control center of the power grid and the smart meter, it is proved that a statistical analysis approach cannot protect the system from false data injection attack [11]. It would also be infeasible for the smart grid system to adopt this approach since the system will need to handle a large amount of data in real time, but the control center of the smart grid system only has a few seconds to respond.

Some solutions have been proposed in [12], [13], [14] and [15]. All these works provide user authentication. The schemes proposed in [12] and [13] even provide some level of user privacy preservation. [12] assumes that the power operator is fully trusted and can know the electricity usage pattern of all customers. [13] does not allow the power operator to know the electricity usage pattern of any customer. Their work also adopts anonymous credentials as in our scheme. However, their use of credentials with many different values causes huge burden to both the control center as well as the communications network during the registration phase. Nevertheless, none of the works address the power selling issue.

3 System Model and Security Requirements

Following [12] and [13], we assume that a smart gird network can be simplified into three basic layers to form a hierarchical structure. At the top level, there is a control center maintained by the power operator. At the second level, there are substations in the distribution network and each substation is responsible for the power supply of an area. At the lowest level, there are smart meters which are placed at the homes of the customers.

Smart meters should send requests to the control center when they want to sell power back to the grid. The control center can be a single server located inside the power plant or be distributed servers located at different geographical locations for load-balancing purposes and to avoid single point of failure. The communication channels from the smart meters to the control center and from the substations to the control center may be the Internet which is public and is always considered unsafe.

We aim at designing a system to resolve the following security problems:

a) Message authentication: Every request message sent by any smart meter should be checked to confirm that it is from a valid user. Authentication is the basis of the system. Without it, anyone can abuse or attack the system easily.
b) Identity privacy preservation: The real identity of the customer during the requesting phase should be unknown to everyone, including the power operator to protect the privacy of customers.
c) Request message confidentiality: The amount of power to be sold to the grid by any smart meter should not be known by any third party in order to protect the privacy of the customers.
d) Traceability: The total amount of power to be uploaded by each customer in a certain period of time should be known by the power operator (i.e. its control center) so that it can compare this value with the smart meter measurement and to arrange payment to the customer accordingly.

4 Details of Our Scheme

In our scheme, we assume that any smart meter can communicate with the control center via a secure communications channel. That is, every message transmitted is encrypted (say using AES encryption) and third parties cannot read the contents without the key concerned. The basic idea of our scheme is to make use of the blind signature technique for the control center to sign credentials on behalf of customers. In this way, when a customer presents a credential anonymously (without any information about the customer's identity provided), the control center cannot tell which customer is making the request, yet it can verify the signature to confirm that it is from a valid customer because only a valid customer can request for blind signatures. At the end of each month, each customer sends the unused credentials back to the control center to evaluate the amount of power he has agreed to sell so far. Next let us describe our scheme in details.

A Setup Phase

During system startup, the control center assigns itself an RSA public and private key pair for signing credentials. The public key is assumed to be known by everyone while the private key is only known by the control center.

Whenever a new smart meter is registered, it will be assigned a unique identity for identification purpose and a secret value for authentication purpose (details of their usage will be discussed later). Also a shared key between the smart meter and the control center, *sk*, will be established.

B Registration Phase

At the beginning of each month, the registration phase will be carried out. *This phase is not anonymous*. Customers need to be authenticated using their real identities in this phase. For this purpose, the smart meter submits its identity and secret value to

the control center (via a secure channel) to authenticate itself. This phase continues with the following steps:

Step 1: Each customer, with the help of the smart meter, sends credential signing requests to the power operator. Each credential C_i is of the format: (*CID*, *date of issuance*, *V*). Recall that *CID* is a unique[1] (it has been shown in [13] that the probability of collision is low if its size is properly set) credential identifier for each credential and *V* indicates that by presenting a credential, one agrees to upload *V* credits of power to the grid.

Step 2: For each credential the smart meter needs, *n* credentials with *n* different *CID*s and blinding factors, where *n* is pre-determined by the control center, are generated. Among them, the control center requests the customer to open $(n - 1)$ of them for verification purpose.

Step 3: If the information in all the "opened" credentials is valid, the control center signs the remaining one. Otherwise, it requires the customer to re-submit its request. Recall that the blinded version of credential C_i constructed by the customer is in the format $B_i = (C_i F_i^e)$ *mod n*, where F_i is the blinding factor. For each signed credential, the control center assigns each blinded credential B_i a unique blinded credential identity, BID_i and stores BID_i, B_i together with the customer's identity into a list L_1 in its local database. Finally, the control center transmits BID_i and its signature on B_i (i.e. $(C_i^d F_i)$ *mod n*) back to the customer.

Step 4: The smart meter extracts the control center's signature, C_i^d *mod n*, on the credential by multiplying the inverse of the blinding factor F_i to the received signature.

Step 5: The smart meter repeats Steps 2 to 4 above until all credentials required have been signed.

Step 6: The smart meter stores BIDs and blinding factors of all signed credentials locally.

Step 7: The control center calculates and records the number of credentials that it has signed so far into its local database.

Step 8: The smart meter of the customer stores these signed credentials properly for later usage. Since a smart meter can be considered as a tamper-proof device, we assume that the stored signed credentials cannot be modified by an outsider easily.

C Power Selling Phase

This phase can be executed at any time during the month when the smart meter of a customer finds that it has excess power to sell back to the grid. To protect the privacy of the customer, *this phase is anonymous*. Customers do not have to authenticate themselves in this phase and the validity of the customer is represented by the anonymous credentials made in the registration phase.

When the customer wants to sell power back to the power grid, the smart meter randomly picks and sends an appropriate amount of credentials to represent the

[1] It has been shown in [12] that the collision probability of *CID*s can be very low if the size of *CID* is properly set.

amount of power uploading agreed. In our design, the value of each credential V is expressed in terms of credits such that the power operator can impose different weights on power sold at different times. For example, a customer can get more revenue if he/she sells power during peak hours. Without loss of generality, assume that the current weight is R credits for each unit of power sold. If a customer wants to sell T units of power, the smart meter has to submit $\lfloor TR/V \rfloor$ credentials to the control center. The control center then verifies its own signature on each credential. It then checks whether the credential identifier *CID* has been used previously and whether *date of issuance* is up to date. To facilitate the former checking, the control center maintains another list L_2 to store all used *CID*s. This list will also be used in the reconciliation phase. A used credential will be considered as invalid. Otherwise, the control center includes this new *CID* into L_2 and broadcasts the list to all customers as an acknowledgement. In this way, a customer can know that its power selling request has been approved by the control center. Each smart meter maintains a list L_3 to record *BID*s and the corresponding blinding factors of credentials in all approved power selling instances.

For each used credential C_i, the smart meter generates a keyed hash on the identity of the blinded credential, BID_i, together with the random blinding factor used, F_i. The key used here is the shared key, sk, established between the customer and the control center in the setup phase. That is, the keyed hash is of the format $h_{sk}(BID_i, F_i)$. All these keyed hash values are stored into a list L_4. Both lists L_3 and L_4 will be used in the reconciliation phase.

D Reconciliation Phase

After a certain time period (e.g. at the end of a month), the reconciliation phase will be carried out. Similar to the registration phase, *this phase is not anonymous*. Customers need to be authenticated using their real identities in this phase.

Assume that a customer has used n credentials for which the *BID*s and the corresponding blinding factors are recorded in the list L_3 in the smart meter. The list L_4 stores n keyed hash values accordingly.

In the reconciliation phase, the smart meter sends the list L_4 to the control center. Upon receiving L_4, the control center randomly picks m, where $m < n$, entries from L_4 to form a sub-list L_5. The control center then challenges the smart meter to reveal entries in L_5 by providing the m *BID*s and the m blinding factors concerned. Upon receiving the response, the control center re-computes m keyed hash values with the received *BID*s and blinding factors to see whether they are the same as those listed on L_5. On the other hand, the control center also checks whether the *BID*s actually belong to that particular customer by checking their existence in list L_1 in its local database. If both checking pass, for each pair of BID_i and F_i, the control center tries to use the blinding factor F_i to "open" the blinded credential B_i with identifier BID_i (i.e. to compute $C_i = (B_i / F_i^e) \bmod n$). This is possible because all blinded credentials have been stored in list L_1 during the registration phase. After obtaining the actual credential C_i which is of the format $C_i = (CID_i, \textit{date of issuance}, V)$, the control center checks whether CID_i has been used by checking its existence in the list L_2. If all the m opened credentials are

valid, the control center assumes that the remaining $(n - m)$ unopened credentials are also valid. The control center then trusts that the customer has sold nV credits of power to the grid during the month, and later offers payments to the customer.

5 Security Analysis

In this section, we evaluate our scheme according to the security requirements listed in Section 3:

a) Message authentication: During the registration phase, a customer needs to authenticate himself/herself using the private key signature before requesting any signing of credentials. So when the customer presents the signed credentials during the power selling phase, he/she proves himself/herself authenticated.
b) Identity privacy: Customers only reveal their identities during the registration and the reconciliation phases. During the power selling phase, when the customer presents the credentials, the control center only knows whether the credential is from a valid user or not. Due to the properties of the blind signature, the credential identity is only known by the owner. The credentials do not reveal the identities of the customers.
c) Request message confidentiality: As we mentioned earlier, we assume that a smart meter communicates with the control center via a secure channel. Therefore, the amount of power to be sold agreed by any smart meter cannot be known by any third party. Confidentiality of the request message is preserved.
d) Traceability: During the registration phase, a customer needs to present his/her identity (i.e. not anonymous) to obtain signed anonymous credentials. In the reconciliation phase, a customer again needs to present his/her identity to the control center. Therefore, the total amount of power requested by each particular customer in a certain period of time (say a month) can be known by the control center. The control center can then properly offer payments to the customer at the end of the billing period.

6 Conclusion

In this paper, we focused on how to facilitate a customer to sell power back to the power grid in a secure and privacy-preserving manner. We proposed a secure and privacy-preserving protocol to solve the problem. Basically, we adopted the technique of anonymous credentials for authentication. These credentials are generated by the customer but are blindly signed by the control center. Also based on our design, even in the reconciliation phase, the power operator only knows how much power a customer has sold to the grid but cannot tell when the customer has done so. We evaluated our scheme using security analysis to show that it is effective. In the future, we will investigate the tradeoff between privacy preservation and traceability statistically, suggest how to set the proportion of credentials that the control center should choose for challenging in the reconciliation phase, and study other security problems in smart grid.

Acknowledgement. This research is supported in part by the HKU RCGAS Small Project Funding under Grant No. 201109176206, the Collaborative Research Fund of the Research Grants Council of Hong Kong under Grant No. HKU10/CRF/10, the General Research Fund from the Research Grants Council of the Hong Kong Special Administrative Region, China under Project No. RGC GRF HKU 713009E and the NSFC/RGC Joint Research Scheme under Project No. N_HKU 722/09.

References

1. Networx: Guide to Selling Power Back to the Grid, http://www.networx.com/article/guide-to-selling-solar-geothermal-and
2. Khurana, H., Hadley, M., Lu, N., Frincke, D.A.: Smart-Grid Security Issues. IEEE Security and Privacy Magazine 81–85 (2010)
3. The Smart Grid Interoperability Panel Cyber Security Working Group: Second Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements (2010)
4. Office of the National Coordinator for Smart Grid Interoperability: NIST Special Publication 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (2010)
5. SmartGrids: European SmartGrids Technology Platform: Vision and Strategy for Europe's Electricity Networks of the Future. In: European Commission, Directorate-General for Research, Sustainable Energy Systems, EUR 22040 (2006)
6. Electric Power Research Institute: Intelligrid, http://intelligrid.epri.com/
7. US Department of Energy: Grid 2030: A National Vision for Electricity's Second 100 Years (2003)
8. Wen, M.H.F., Leung, K.C., Li, V.O.K.: Communication-oriented Smart Grid Framework. In: Proceedings of the IEEE SmartGridComm 2011 (2011)
9. Li, V.O.K., Wu, F.F., Zhong, J.: Communication requirements for Risk-Limiting Dispatch in Smart Grid. In: Proceedings of the IEEE Workshop on Smart Grid Communications (2010)
10. Liu, Y., Ning, P., Reiter, M.K.: False Data Injection Attacks against State Estimation in Electric Power Grids. In: Proceedings of the CCS 2009, pp. 21–32 (2009)
11. Chim, T.W., Yiu, S.M., Hui, Lucas C.K., Li, V.O.K.: PASS: Privacy-preserving Authentication Scheme for Smart Grid Network. In: Proceedings of the IEEE SmartGridComm'11 (2011).
12. Cheung, J.C.L., Chim, T.W., Yiu, S.M., Hui, L.C.K., Li, V.O.K.: Credential-based Privacy-preserving Power Request Scheme for Smart Grid Network. In: Proceedings of the IEEE GLOBECOM 2011 (2011)
13. Fouda, M.M., Fadlullah, Z.M., Kato, N., Lu, R., Shen, X.S.: Towards a Light-weight Message Authentication Mechanism Tailored for Smart Grid Communications. In: Proceedings of the First International Workshop on Security in Computers, Networking and Communications, pp. 1018–1023 (2011)
14. Fouda, M.M., Fadlullah, Z.M., Kato, N., Lu, R., Shen, X.S.: A Lightweight Message Authentication Scheme for Smart Grid Communications. IEEE Transactions on Smart Grid 2(4), 675–685 (2011)