A privacy protection scheme based on certificateless aggregate signcryption and masking random number in smart grid

Juqin Chen, Xiaoxi Ren
College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

ABSTRACT: Security of data transmission and privacy protection are key issues in smart grid. Aiming at the improvement of the above issues, a privacy protection scheme is proposed based on certificateless aggregate signcryption and masking random number. In the proposed scheme, the building gateways generate masking random matrix satisfying requirements, according to time sharing billing strategy sent by control center, and then send the matrix to users. The data of users send to building gateway after adding masking random number and signcryption and the building gateway send data to the control center after aggregate signcryption. Then, the control center saves data after verifying and unsigncrypt. Theoretical study and security analysis indicates that the proposed method reduces the communication cost and simplifies the procedure of encryption and decryption.
KEYWORD: Smart grid, Communications Security, Privacy protection, Masking random number, Certificateless aggregate signcryption.

1 INTRODUCTION

In the smart grid, the fine-grained electricity data collected by smart meters can reveal the users' privacy (Lisovich, 2010), such as the user's living habits and hobbies, etc. So the term of privacy and authentication are becoming of high interest and much discussed. In order to prevent illegal users access or tamper with the data resources, and protect the safety of the smart grid, the transmit message should be encrypted and authenticated in smart grid. In addition, the high frequency of vast amounts of transmission, an efficient data encryption and authentication scheme is necessary in smart grid.

Zhang (Zheng Yuliang, 1997), et al. propose the signcryption method at the earliest. The signcryption can accomplish the functions of digital signature and public key cryptography within a reasonable logical step. Its computation and communication costs are lower than the traditional sign-then-encrypt. In 2008, Barbosa (Barbosa M, 2008), et al. present the concept of certificateless signcryption firstly and many certificateless signcryption scheme agreements are proposed (Sun Yin-xia, 2010). However, when the signcryption amount is biger, a normal signcryption scheme is inefficiency. Aggregate signcryption(Boneh D, 2003) can gather more than one ciphertexts and provide batch quantity verification. The efficiency of communication transmission and signcryption verification is improved. Certificateless aggregate signcryption not only can solve problems of certificate management of traditional public key cryptography and key escrow of identify public key cryptography. Meanwhile, the cost of signature verification and correspondence can be reduced. To improve the correspondence and calculation efficiency of smart grid, it is necessary to transfer the ciphertext aggregately and verify the ciphertext.

This paper proposes a privacy protection scheme based on masking random number and certificateless aggregate signcryption. Before the users send data, the masking random number sent by the building gateway is added and the data are sent to the building gateway after signcryption. Then, the building gateway sends data to the control center after aggregate signcryption. Finally, control center recover data which contains masking random number and save it.

2 SYSTEM MODEL

As a premise, network model of the smart grid is understood as hierarchical network in this paper, including power control center (CC, for short), building gateway (BG, for short) and users (Shown in Fig.1). Assuming that the power control center can cover m building gateways and each building gateway is consisted of n user networks. Moreover, each user distributes an automation smart meter to realize

bidirectional communication between the BGs and users. The control center and building gateway are considered as credible units. The control center is responsible for system initialization, generating system parameters, registering of building gateway, information and key management, verifying non-repudiation and integrity of information, decryption and dealing with aggregation and releasing the response message. On the other hand, building gateway is responsible for registering of users, information and key management and gathering data of users and uploading to control center.

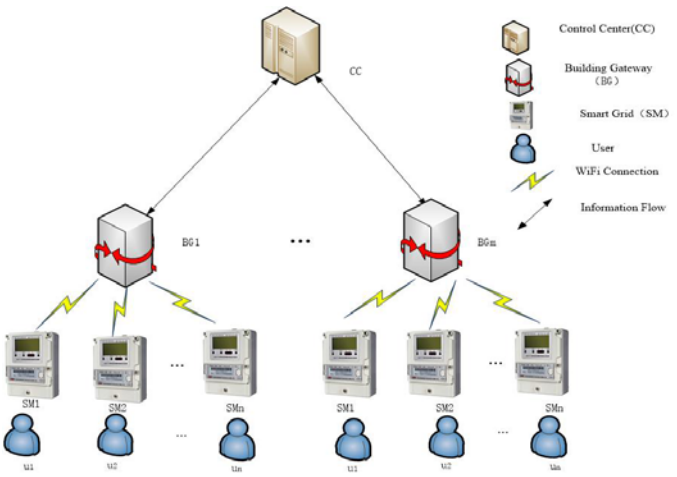

Fig.1 Network model for smart grid

3 SCHEME DESCRIPTION

In this paper, a privacy protection scheme of smart grid based on masking random number and certificateless aggregation is proposed. The scheme consists of the following 7 parts:

3.1 System Initialization.

1) CC selects a safty parameter k, q is a large prime number, G1, G2 are cyclic group of the same order q, P is a generator of G1. The bilinear pairing is a map $\hat{e}: G_1 \times G_1 \to G_2$.Define three hash function: $H_1, H_3, H_4: \{0,1\}^* \times G_1 \to G_1$, $H2:\{0,1\}^* \to \{0,1\}^{l_m}, H5:\{0,1\}^* \to Z_q^*$, l_m is for message bit length. 2) CC selects a random number $s \epsilon z_q^*$ for master key, and set $P_{pub} = sP$ as its public key. System public parameters

$$Params = \{G_1, G_2, q, \hat{e}, P, P_{pub}, H_1, H_2, H_3, H_4, H_5\}.$$

CC sends time billing cycle T to the building gateway.

3.2 Generation of Masking Random Numbers.

BG generates a r*n two-dimensional matrix $A=\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{r,1} & \cdots & a_{r,n} \end{pmatrix}$ (r=T/t) according to the time-sharing billing cycle T, measuring time interval t and the number of users n in each building. The two-dimensional matrix A meets the two following conditions: the sum of each row of the matrix is zero while the sum of each column is zero as well.

3.3 Generation of Users' Key.

1) CC calculates the value of $Q_i = H_1(ID_i)$ and $D_i = sQ_i$. Di is transmitted to the user and the corresponding building gateway through a secure channel. 2) User u_i chooses $x_{ID_i} \in_R Z_q^*$ as a part of private key and calculates its value of public key $P_{ID_i} = x_{ID_i} P$. So, the value of the private key of user u_i is $S_{ID_i} = (x_{ID_i}, D_i)$,the public key is P_{ID_i}.

3.4 Generation of Users' Message.

Identity of the user ui is IDi. The public key is P_{ID_i} and the private key is S_{ID_i}. Masking random number is $a_{j,i}$. mj,i is the electricity data for the measurement t. Identity of control center is IDR and the the public key of it is P_R. The user performs the following operations:

1) Choosing $r_i \in_R Z_q^*$ and calculating the value of $R_i = r_i P, Q_R = H_1(ID_R)$ and $T_i = \hat{e}(P_{pub}, Q_R)^{r_i}$.

2) Calculating $V_i = H_2(R_i, T_i, r_i P_R, ID_R, P_R)$, $m'_{j,i} = m_{j,i} + a_{j,i}$ $C_i = V_i \oplus m'_{j,i}$.

3) Calculating $\phi = H_3(P_{pub}), \varphi = H_4(P_{pub}), h_i = H_5(R_i, ID_i, P_i, ID_R, P_R)$.

4) Calculating $S_i = D_i + h_i r_i \phi + x_i \varphi$.Then, the signcryption ciphertext $\delta_i = (R_i, C_i, S_i)$ is sent to the building gateway.

3.5 Aggregate Signcryption.

The building gateway calculates $\varphi = H_4(P_{pub})$ according to the system public parameter Params, the identity list IDi of the corresponding sender ui, the public key list, the message mj,i of corresponding cipher text $\delta_i = (R_i, C_i, S_i)$, the control center of the identity of IDR and the public key PR, then, the value of aggregated cipher is: $\delta = (R_1, R_2, ..., R_n, C_1, C_2, ..., C_n, S)$.

3.6 Unsigncryption.

The following steps are carried out to decrypt the aggregated signcryption after the control center receives the aggregated signcryption transmitted by the BG:

1) Calculate $\phi = H_3(P_{pub})$, $\varphi = H_4(P_{pub})$, $h_i = H_5(R_i, C_i, ID_i, P_{ID_i}, ID_R, P_R), Q_i = H_1(ID_i)$.

2) Verify whether the equation $\hat{e}(S,P) = \hat{e}\left(\sum_{i=1}^{n} Q_i, P_{pub}\right)\hat{e}\left(\sum_{i=1}^{n} h_i R_i, \phi\right)\hat{e}\left(\sum_{i=1}^{n} P_i, \varphi\right)$ is holds or not. If it is not established, then reject the signcryption. If established, continue to carry out the following steps:

a). Calculating $T_i = \hat{e}(R_i, D_R)$, $V_i = H_2(R_i, T_i, x_R R_i, ID_R, P_R)$.

b). Calculating $m_{j,i} = V_i \oplus C_i$ and $m'_{j,i}$ is obtained.

3.7 Storage of Users' Data.

CC stores the user's data m'j,i respectively according to the ID_i.

4 SECURITY ANALYSIS

4.1 Correctness.

Theorem 1. The scheme is correct in this paper.

Prove: In this scheme, only when the signed secret cipher $\delta_i = (R_i, C_i, S_i)$ and the aggregated signcryption $\delta = (R_1, R_2, ..., R_n, C_1, C_2, ..., C_n, S)$ are calculated by the correct algorithm of the signature algorithm, the method can be verified. And there are three kinds of validation equation was established:

1) BG can verify the correctness of $\delta_i = (R_i, C_i, S_i)$.

$$\hat{e}(S_i, P) = \hat{e}(D_i + h_i r_i \phi + x_i \varphi, P) = \hat{e}(D_i, P)\hat{e}(h_i r_i \phi, P)\hat{e}(x_i \varphi, P) = \hat{e}(Q_i, P_{pub})\hat{e}(h_i R_i, \phi)\hat{e}(P_{ID_i}, \varphi)$$

2) CC can verify the correctness of $\delta = (R_1, R_2, ..., R_n, C_1, C_2, ..., C_n, S)$:

$$\hat{e}(S, P) = \hat{e}\left(\sum_{i=1}^{n} S_i, P\right) = \hat{e}\left(\sum_{i=1}^{n} Q_i, P_{pub}\right)\hat{e}\left(\sum_{i=1}^{n} h_i R_i, \phi\right)\hat{e}\left(\sum_{i=1}^{n} P_i, \varphi\right) = \hat{e}\left(\sum_{i=1}^{n} Q_i, P_{pub}\right)\hat{e}\left(\sum_{i=1}^{n} h_i R_i, \phi\right)\hat{e}\left(\sum_{i=1}^{n} P_i, \varphi\right)$$

3) CC can decrypt C_i correctly. Control center calculates V'_i:

$$V'_i = H_2(R_i, T_i, x_R R_i, ID_R, P_R) = H_2(R_i, \hat{e}(R_i, D_R), x_R r_i P, ID_R, P_R) = H_2(R_i, \hat{e}(r_i P, sQ_R), x_R r_i P, ID_R, P_R)$$

At the same time, due to:

$$V_i = H_2(R_i, T_i, r_i P_R, ID_R, P_R) = H_2(R_i, \hat{e}(P_{pub}, Q_R)^{r_i}, r_i P_R, ID_R, P_R) = H_2(R_i, \hat{e}(sP, r_i Q_R), r_i x_R P, ID_R, P_R)$$

Therefore, the formula $m'_{j,i} = V'_i \oplus (V_i \oplus m'_{j,i}) = m'_{j,i}$ is established. Therefore, the control center can obtain user's data, which contains the masking random number.

4.2 The Confidentiality of Users' Data.

The security of our proposed scheme is based on the signcryption. Hence, eavesdroppers cannot obtain any information from the data transmission packets without the keys of user and CC, even though they can observe them. Moreover, the ciphertexts do not reveal any information of original data since the signcryption uses different random numbers r_i for encryption every time. What's more the CC store $m_{j,i}$ as the users' datas ,which contains the masking random number , eavesdroppers can't get the real information .

4.3 Efficiency Analysis.

In this section, we analyze the efficiency of schemes mainly in three aspects. It is the computation costs for signcrypt, aggregate verify and Designcrypting operations. The comparison of (Jiang Yi, 2013) schemes are displayed in Table 1. P means the multilinear pairing computation, n is the number of user in BG.

Observation from the table 1, we can see that the computation costs of our scheme is lower than the scheme of (Jiang Yi, 2013).

Table 1 Efficiency Comparison of Aggregate Signcryption Schemes

Scheme	Signcrypt	Aggregation verify	Designcrypting
Scheme of smart grid	nP	(2n+1)P	4nP
Our Scheme	nP	4P	nP

5 SUMMARY

This paper proposes a privacy protection scheme based on certificateless aggregate signcryption and masking random number. Masking random numbers can mask users' real power consumption data, certificateless aggregate signcryption can keep the users' data confidential and authenticated. Through theoretical analysis, the scheme can reduce communication overhead encryption and decryption process and protect the privacy of user in the smart grid at the same time.

ACKNOWLEDGMENTS

This paper was supported by Science and Technology Planning Project of Hunan Province, China (2015JC3054).

REFERENCES

Barbosa M and Farshim P. Certificateless signcryption[C]. Proceedings of the ASIACCS2008, New York, USA, 2008: 369-372

Boneh D, Gentry C, Lynn B, et al.. Aggregate and verifiably encrypted signatures from bilinear maps[C]. Proceedings of the Cryptology–EUROCRYPT2003, Warsaw, Poland, 2003: 416-432

Guang Yan, Gu Chun-xiang, Zhu Yue-fei, et al.. Certificateless fully homomorphic encryption based on LWE problem[J]. Journal of Electronics & Information Technology, 2013, 35(4): 988-993. [7] Zhou Cai-xue, Zhou Wan, and Dong Xi-wei. Provable Certificateless generalized signcryption scheme[J]. Designs, codes and Cryptography, 2014, 1(2): 331-346.

Jiang Yi, Li Jian-ping, and Xiong An-ping. Certificateless aggregate signcryption scheme for wireless sensor network[J]. International Journal of Advancements in Computing Technology, 2013, 5(8): 456-463.

Lisovich, Mikhail A., D. K. Mulligan, and S. B. Wicker. Inferring Personal Information from Demand-Response Systems. IEEE Security & Privacy Magazine 8.8(2010):11-20.

Ming Yang, Zhao Xiang-mo, and Wang Yu-ming. Certificateless aggregate signature scheme[J]. Journal of University of Electronic Science and Technology of China, 2014, 43(2): 188-193.

Sun Yin-xia, Li Hui, and Li Xiao-qing. Certificateless signcryption KEM to multiple recipients[J]. Journal of Electronics & Information Technology, 2010, 32(9): 2249-2252.

Shi Wen-bo, Kumar N, Gong Peng, et al.. Cryptanalysis and improvement of a certificateless signcryption scheme with-

out bilinear pairing[J]. Frontiers of Computer Science, 2014, 8(4): 656-666.

Weng Jian, Yao Guo-xiang, Robert Deng, et al.. Cryptanalysis of a certificateless signcryption scheme in the standard model[J]. Information Science, 2011, 181(3): 661-667.

Zheng Yuliang. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption) [C]. Advances in Cryptology-CRYPTO. Berlin: Springer-Verlag, 1997: 165-179