Internet of Things (IoT) and Engineering Applications (2019) 4: 7-12
Clausius Scientific Press, Canada
DOI: 10.23977/iotea.2019.41002
ISSN 2371-8617

Research on Privacy Protection Scheme Based on Certificateless Aggregation Signcryption in AMI

Wang Baoyi[a,*], Liu Li[b], Zhang Shaomin[c], Huang Jing

School of Control and Computer Engineering, North China Electric Power University, Baoding, 071003, China

[a]email: wangbaoyiqj@126.com, [b]email:2529333628@qq.com, [c]email:zhangshaomin@126.com

Keywords: AMI, certificateless aggregation signcryption, privacy protection

Abstract: User's power smart meter value is frequently uploaded to the power company by the smart meters, which makes users face privacy leakage issues. The smart meter sends the data to the power company through the data concentrator. So the data concentrator has a large amount of data to be transmitted. Therefore, we design a secure certificateless aggregation signcryption scheme for this problem. Using the scheme not only protects the user's power usage information from being leaked, but also reduces the amount of data transmitted by the data concentrator by aggregation. Through calculation and comparison, it is concluded that implementing the scheme has shorter computing time than the existing security scheme, which can greatly improve the data transmission efficiency.

1. Introduction

In the Smart Grid, Advanced Metering Infrastructure (AMI) is an important part[1]. Power company can obtain comprehensive ability of the entire smart grid from the AMI[2]. AMI is the basis for interacting between the power company and the power user and optimizing the allocation of resources [3].

AMI is mainly composed of smart meter(SM), home area network, local communication network, communication network that connects power companies, and measurement data management system(MDMS)[3]. Smart meter is an important part of AMI, and it is also the most important component of the user side in smart grid. It differs from the traditional meter in that the smart meter has the functions of remote reading and two-way communication. Smart meters can record power consumption value every few minutes and send it back to the power company for real-time monitoring management and real-time pricing[4].

The large-scale data collection of smart meters makes users face the problem of privacy leakage. After obtaining a large amount of power consumption data, the attacker can not only sell the information to obtain direct economic benefits, but also analyze the user's power consumption characteristics through data mining technology to carry out further crimes. Therefore, choosing the appropriate encryption technology plays an important role in the uplink network of AMI, providing better privacy and security for consumer data. For the privacy protection issue, many security schemes[5-7] have been proposed. In the literature[1], the author designed a key management mechanism for the unicast and multicast communication based on the information transmission

method in AMI. In the literature [5], for the case of limited computing and storage resources of embedded devices such as smart meters, a Blom key negotiation mechanism including a trusted third-party key management center was introduced by the researchers. However, due to the scalability and complexity, the use of public key infrastructure (PKI) and certificates and certification authorities (CA) is unpopular in the smart grids [6].

The aggregation signcryption scheme in the field of information security can combine multiple signcryption ciphertexts and perform batch verification, which is very suitable in the multi-to-one mode of distributed communication with high energy consumption and real-time requirements [8]. Therefore, the design of a secure and efficient integrated signcryption scheme[9-10] has become a research hotspot. In the AMI, the computing resources of the smart meter are limited, and the metering data is frequently uploaded to the data concentrator, and the data concentrator uploads the measured values of the plurality of smart meters to the power company, and the amount of data is very large. Therefore, in view of this feature, this paper improves the existing certificateless aggregation signcryption scheme, so that the scheme does not involve complex operations and meets data security requirements.

2. Proposed Scheme

According to the characteristics of measurement value transmission in AMI, in this paper, we design a certificateless signcryption mechanism to ensure the security of information transmission.

The structure of the AMI system is shown in Figure 1.

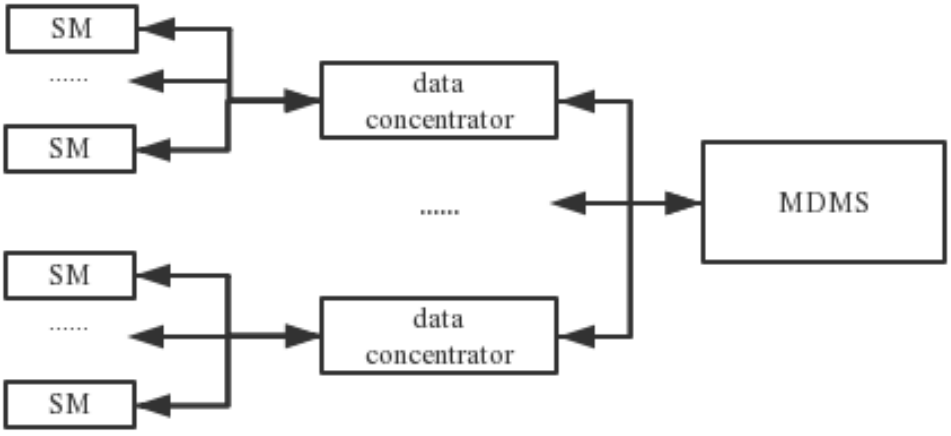

Figure 1: AMI system structure.

As shown in the Figure 1, the process of uploading information is that the smart meter uploads the user's power consumption value to the data concentrator, and the data concentrator uploads the information to the measurement data management system. The process of transmitting instructions from measurement data management system is reversed. In this paper, we only consider the security of uploading information, and the security of the downloaded instructions is described in another paper. In our designed scheme, a high-performance and mass-storage computing device as a trusted third-party KGC is introduced in the data communication of AMI. KGC can generate partial public key and partial private key of smart meter and data concentrator. For the process of uploading the user's electric power information, the smart meter sends the information to the data concentrator, and the data concentrator uploads the received values of the plurality of smart meters to the measurement data management system. After receiving the information, measurement data management system verifies the information, and the power consumption information of each user can be obtained after the verification is passed.

The aggregation signcryption mechanism designed in this paper includes six basic algorithms. We combine part of the key generation algorithm and public key generation algorithm into the user key generation algorithm. Therefore, the six basic algorithms are system initialization algorithm, user key generation algorithm, signcryption algorithm, aggregation signcryption algorithm, aggregation signcryption verification algorithm and unsigncryption algorithm. The specific steps are as follows.

2.1. System Initialization Algorithm

During the system initialization phase, KGC performs the following operations.

1) The order of the cyclic group G is a large prime number q, P is a generator of G. KGC selects the following anti-collision hash functions which ensure that the hash function has different outputs for different inputs.

$H_1:\{0,1\}^{l1}\times G\times G\rightarrow Z_q^*$, $H_2:\{0,1\}^{l1}\times\{0,1\}^{l2}\times G\times G\rightarrow Z_q^*$, $H_3: G\rightarrow Z_q^*$.

where *l1* is the length of the identity *ID*, and *l2* is the length of the electric power consumption information.

2) KGC randomly selects $S\in Z_q^*$ as the master key and keeps it secretly, then calculates $P_{pub}=SP$, where P_{pub} is the system master public key. Then the system parameters $Par=(q, G, P, P_{pub}, H_1, H_2, H_3, ID, M)$ is pubic.

2.2. Key Generation Algorithm

The key generation process of the smart meter (ID_i) is as follows.

1) The secret value $s_i\in Z_q^*$ is selected and public parameters S_i is calculated by the node named ID_i, the calculation method of S_i is $S_i=s_iP$. Then ID_i and S_i are sent to KGC, where ID_i and S_i are the identity information and public parameters, respectively.

2) Receiving ID_i and S_i, KGC randomly selects $r_i\in Z_q^*$ as the secret number and calculates $T_i=r_iP$ and $t_i=r_i+SH_1(ID_i, S_i, T_i)$. Then KGC returns t_i and *Ti* to ID_i over a secure channel. So the PK_i is (S_i, T_i) and the SK_i is (s_i, t_i), where PK_i and SK_i are the public key and private key, respectively. The smart meter or data concentrator gets its own public key and private key and saves it. The smart meter can verify the legitimacy of the distribution of the key by whether the equation (1) holds.

$$t_iP= T_i+ P_{pub}\, H_1(ID_i, S_i, T_i) \qquad (1)$$

2.3. Signcryption Algorithm

When the smart meter(the identity is ID_i) wants to send message *m* to the data concentrator, it performs the following operations.

1) The smart meter firstly picks up secret number $u_i\in Z_q^*$ and calculates $Q_i=u_iP$ and $W=u_i(S_B + T_B + P_{pub}h_B)$, where $h_B = H_1 (ID_B , S_B , T_B)$. Then the ciphertext C_i is generated and $C_i= m\oplus H_3(W)$, where ID_B represents the measurement data management system node that ultimately receives the message.

2)Then the smart meter calculates $n_i=H_2(ID_i,C,S_i, Q_i)$ and $k_i=H_2(ID_i, C_i,T_i, Q_i)$, so the signature $V_i = n_i(s_i + t_i) + u_ik_i$ is generated.

3) The ciphertext σ is generated, and the content is (Q_i, V_i, C_i) and sent to the data concentrator by the smart meter.

2.4. Aggregation Signcryption Algorithm

After the data concentrator receives the message sent by multiple smart meters in the area, it calculates $V = \sum_{i=1}^{n} V_i$. Then the data concentrator sends the message $\beta=(Q_1, Q_2,\ldots\ldots, Q_i, C_1, C_2,\ldots\ldots, C_i,V)$ to measurement data management system.

2.5. Aggregation Signcryption Verification Algorithm

After the measurement data management system receives the ciphertext sent by the data concentrator, the following operations are performed. The equation VP is computed. If the equation (2) is established (where $h_i = H_1(ID_i, S_i, T_i)$, $n_i = H_2(ID_i, C_i, S_i, Q_i)$, $k_i = H_2(ID_i, C_i, T_i, Q_i)$), it is inferred that the aggregation signcryption is valid. Otherwise, the aggregation signcryption is not correct, and the message is not received by the measurement data management system.

$$VP = \sum_{i=1}^{n}[n_i(S_i + T_i + P_{pub}h_i) + k_iQ_i] \quad (2)$$

2.6. Unsigncryption Algorithm

If the aggregation signcryption verification algorithm is passed, the measurement data management system uses its own private key to calculate $W'=(s_B+t_B)Q$ and recovers the plaintext message *m* and the calculation method is $m=C\oplus H_3(W')$.

3. Security Analysis and Efficiency Analysis

3.1. Correctness Analysis

In the key generation algorithm of section 2.2, the node ID_i verifies the legitimacy of the KGC distribution key by the following equation (3).

$$t_iP= (r_i+SH_1(ID_i, S_i, T_i))P=T_i+ SPH_1(ID_i, S_i, T_i)= T_i+ P_{pub}\ H_1(ID_i, S_i, T_i) \quad (3)$$

In the aggregation signcryption verification algorithm of section 2.5, the measurement data management system verifies the correctness by the equation (4).

$$VP=\sum_{i=1}^{n}(n_i(s_i + t_i) + u_ik_i)P=\sum_{i=1}^{n}(n(S_i + T_i + P_{pub}H_1(ID_i, S_i, T_i)) + u_ik_iP) =\sum_{i=1}^{n}[n_i(S_i + T_i + P_{pub}h_i) + k_iQ_i] \quad (4)$$

In the Unsigncryption algorithm of section 3.6, the measurement data management system verifies the correctness of the message by the equation (5).

$$W'=(s_B+t_B)Q=u(s_B+ t_B)P=u(S_B + T_B + P_{pub}\ H_1(ID_B, S_B, T_B))= u(S_B + T_B + P_{pub}h_B)=W \quad (5)$$

So, the plaintext message is verified, $m=C\oplus H_3(W')= m\oplus H_3(W)\oplus H_3(W')=m$, which illustrates that the message is decrypted correctly by the measurement data management system.

3.2. Unforgeability

Since the certificateless signcryption mechanism faces two types of adversary attacks, we analyze the forgery attacks of two types of adversaries in this section.

A forged attack by the attacker A_I. The attacker A_I can replace the public key of a legitimate user. If the legal public key PK_i is replaced with PK_i', an error occurs in the equation (2) during the aggregation signcryption verification phase. Because the legitimate user's public key is T_i and the

calculation method is $T_i = r_iP$, the attacker cannot calculate r_i, which is a mathematical hard problem in solving the discrete logarithm. Therefore, the scheme designed in this paper can resist the forgery attack by the attacker A_I.

A forged attack by the attacker A_{II}. The attacker A_{II} cannot replace the public key of a legitimate user, but it masters the master key of the system. If the attacker A_{II} wants to forge the message, it needs to calculate the partial private key s_i of the legitimate user. From the above content, we can know that $S_i = s_iP$. And solving s_i is a mathematical hard problem to solve the discrete logarithm. Therefore, the scheme designed in this paper can resist the forgery attack by the attacker A_I.

3.3. Integrity of the Message

In the scheme, the message to be sent, the public key of the measurement data management system and the secret number selected by the smart meter are hashed using a hash function H_3 to ensure that the information is not tampered with.

3.4. Efficiency Analysis

This section analyzes the solution in terms of computational efficiency. Table 2 gives a comparison of the schemes of this paper with other existing schemes. The computational overhead depends mainly on the amount of computation of the signcryption algorithm and unsigncryption algorithm, and *n* represents the number of smart meters in the area.

In this paper, M is used to represent the point multiplication operation on the group, N is the inverse operation, I is the exponential operation on the group, and B is the bilinear pair operation. And the operation time is compared as follows. The relationship is B>I,B>M,M>N.

Table 2: Comparison of various schemes.

scheme	signcryption	unsigncryption
Literature [6]	mI	mI
Literature [8]	nB+3nM	(2n+2)B+nM
Literature [10]	（2n+1）M	4nM
[our scheme]	（2n+1）M	3nM

4. Conclusions

The certificateless aggregation signcryption integrates the encryption into the signature process, and combines multiple signature ciphertexts for batch verification, which improves the communication efficiency of communication. In this paper, we design a certificateless aggregation signcryption scheme for the problem of privacy leakage in AMI, which not only protects the user information, but also reduces the amount of data transmitted by the data concentrator through aggregation.

References

[1] LIANG Jianquan, JIN Xianji, TONG Weiming, et al. Key Management Scheme for Wireless Sensor Networks in Advanced Metering Infrastructure[J].Automation of Electric Power Systems,2016,40(19):119-126.

[2] SU Sheng, LI Zhiqiang, GU Ke, et al. Cloud Security Based Malware Detection in Advanced Metering Infrastructure[J].Automation of Electric Power Systems,2017,41(5):134-138.

[3] LUAN Wenpeng , WANG Guan , XU Daqing. Advanced Metering Infrastructure Solution Supporting Multiple Services and Business Integration [J]. Proceedings of the CSEE, 2014, 34 (29): 5088-5095.

[4] ZHANG Xu. The research on data privacy protection for user in smart grid[D]. Shanghai University of Electric Power, 2017.
[5] LU Baohui, MA Yonghong. Research on communication system of advanced metering infrastructure for smart grid and its data security measures [J]. Power System Technology, 2013, 37 (8): 2244-2249.
[6] V. Seferian, R. Kanj, A. Chehab and A. Kayssi, "Identity Based Key Distribution Framework for Link Layer Security of AMI Networks," in IEEE Transactions on Smart Grid, 2018, 9(4): 3166 - 3179.
[7] FAN Ai-wan,LIU Yukun, ZHAO Weiting. Application of Certificateless Signcryption Scheme to Smart Grids [J]. Electric Power, 2014,47(7):128-133.
[8] LIU J H, MAO K F, HU J W. Certificateless aggregate signcryption scheme based on bilinear pairings[J]. Journal of Computer Applications, 2016, 36 (6): 1558 -1562.
[9] ZHANG X F, WEI L X, WANG X Z. Certificateless aggregate signcryption scheme with public verifiability [J]. Journal of Computer Applications, 2013,33(7) : 1858 -1860.
[10] SU Jingfeng, LIU Juxia. Efficient certificateless aggregate signcryption scheme without bilinear pairings [J]. Journalof Computer Applications, 2018, 38(2): 374-378, 385.