A Lightweight Secure Access Protocol for Collecting Terminals in Power Internet of Things based on Symmetric Cryptographic Algorithm

Zhao Yingjie1*, Zhai Feng1, Liang Xiaobing1, Miao Siwei1 and Zhu Yayun1

1 China Electric Power Research Institute, Beijing, 100192, China
*Corresponding author’s e-mail: zhaoyj@epri.sgcc.com.cn

Abstract. In the development of Power Internet of Things, the types and number of terminals accessing to the power grid information network are growing rapidly, and the demand for identity authentication for master station and terminal is also increasing. This paper analyzes the characteristics and security access requirements of Power Internet of Things, then designs a security access protocol based on symmetric cryptographic algorithm for meters with limited manufacturing cost, computing power and storage resources. This protocol only uses the symmetric cipher algorithm with high computing speed and low resource consumption, which can realize the two-way identity authentication between the meter and the master station and update the session key for meter and master station based on the random initial value of the counter to establish a secure transmission channel. Finally, compared with other protocols, the proposed protocol is also effective in security and performance.

1. Introduction

With the development of information technology, the monitoring and dispatching of power system rely on information technology more and more, such as sensing, communication and artificial intelligence, big data analysis and calculation. Information technology is not only convenient for people to perceive and dispatch the operation state of power grid, but also meet the personalized energy demand of users, but it inevitably brings information security risks. Cryptography is the foundation of information security. It can effectively reduce the risk of illegal access, data theft and tampering by formulating security control mechanism and authentication mechanism.

The costs, computing resources and storage capacity of massive meter devices in the Power Internet of Things are very limited, so the devices cannot meet the high requirements on the resources and performance of the traditional authentication protocol. So, combined with the characteristics of limited resources and capabilities of meters, this paper studies the secure access protocol for lightweight meters in Power Internet of Things based on symmetric cryptographic algorithm to realize the secure and fast access for the massive of power meters in the Power Internet of Things.

2. Related Work

Identity authentication is the first line of defense to ensure the security of the power Internet of things. In order to reduce the security risk brought by malicious terminal access, it is necessary to carry out identity authentication for the collection terminal, which has been studied by many scholars. Some scholars have improved the general Internet security protection method and applied it to power information system. Fu proposed the deployment of industrial firewall, IDS protection equipment
and the use of security protocols. According to Modbus protocol, Fan\cite{5} proposes a scheme of applying deep packet detection in firewall. However, these protocols only protect the information security of power grid by improving the traditional Internet security protection methods, which is not suitable for the power Internet of things with high openness and strong interaction.

Some scholars design the access protocol based on Elliptic Curve Cryptography (ECC). Based on the ECC algorithm, Zhu\cite{6} introduced the concept of trusted certificate authentication agent to reduce the interactive steps in the authentication process. However, the protocol has a large amount of computation and time complexity, which is not suitable for the lightweight requirements of the Power Internet of Things. According to the characteristics of sensor networks Jian and Ding propose\cite{7,8} a key agreement protocol based on ECC is proposed, which has the characteristics of short key length and fast computing speed. However, the methods proposed in the two literatures increase the cost of the public system.

Some scholars use the third-party service to solve the security problem of power grid terminal access to the network. Based on strong identity authentication and Public Key Infrastructure (PKI), Lee\cite{9} designs a mechanism for mutual authentication of smart devices in smart grid, which reduces the message exchange in the authentication process, Yang\cite{10} aims at the security access requirements of a large number of transmission line monitoring terminals, the two-way identity authentication between the terminal and the master station is completed based on PKI. At the same time, asymmetric encryption algorithm is used to update session key. Because of calling the third-party service, the resource consumption of the system is increased.

In addition, Khan\cite{11} proposes a two-way authentication based on hash algorithm, which introduces the shared key and hash algorithm into the authentication process of device access network. The proposed protocol doesn’t establish a secure transmission channel to protect the data.

These above protocols either are improved based on ECC or use the method of calling third-party services. The adaptability of Power Internet of Things is limited, which cannot meet the needs of massive and fast access of the collection terminals. Aiming at the security and fast access requirements for the lightweight terminals, like the meters, this paper studies the security access technology of lightweight terminals based on symmetric cryptographic algorithm.

3. Characteristics and Security Analysis of Power Internet of Things

Due to the combination of power grid and its business requirements, the information system should fully consider its unique characteristics. Figure 1 shows the network architecture of power consumption information collection. The power grid information system has the characteristics of limited resources, different communication time-delay requirements and long equipment operation cycle. The grid equipment mostly adopts the method of embedded security module, which determines that its computing power, memory resources and data transmission speed are limited. The requirements of power grid information system for real-time data change according to the different needs of business, and once the equipment is put into operation, it is difficult to replace or upgrade offline.

Compared with the security requirements of the general Internet, the power grid information system is also quite different. According to the report issued by the National Institute of Standards and Technology of the United States, the priority of information security in general Internet is "Confidentiality > Integrity > Authenticity", but in power grid information system, the priority is "Authenticity > Integrity > Confidentiality". This is because stability and reliability are the first requirements of power system.

According to the above analysis, due to the differences between the power information system and the general Internet system, it is necessary to study the security access protocol which is suitable for the Power Internet of Things to meet the security needs of the rapid access of mass meters.
4. Lightweight Secure Access Protocol based on Symmetric Cryptography

According to the above analysis, this paper designs a lightweight Power Internet of Things security access protocol based on symmetric cipher algorithm to realize the two-way identity authentication between the meter and the master station, and complete the session key update at the same time.

4.1. System Initialization

Security chips are embedded in the current terminals, such as meters and collectors, to store the symmetric key safely. The device completes the symmetric key infusion, random setting of counters and entered the master station information before running. The master station also deploys special security devices to store and use the symmetric key. Besides, it also stores the Identity-Key table of the meters. The secure access protocol proposed in this paper is divided into two parts: Terminal access authentication and Session key updates.

4.2. Terminal Access Authentication

Step1: The meter sends the access authentication request to the master station. The meter generates the random number $N_s$, then encrypts the meter IDs and the random number $N_s$ with the symmetric key $K_s$, and sends $K_s\{\text{IDs}, N_s\}$ and IDs to the master station.

Step2: The master station verifies the identity of the meter, the master station looks up the corresponding key in the Identity-Key table according to IDs and decrypts the massage. Then compares whether the received $ID_s'$ and $ID_s$ are the same. If they are the same, it goes to the step3. Otherwise, it fails.

Step3: The master station shows its identity to the meter. The master station generates the random number $N_c$, encrypts the master station $ID_c$, $N_c$ with $K_s$, and sends $K_s\{ID_c, N_c, N_s\}$ to the master station.

Step4: The meter verifies the identity of the master station. The meter decrypts the massage and verifies the consistency of the decrypted $N_c'$ and $N_c$, the $ID_c'$ and $ID_c$. If they are the same, go to the next step, otherwise the authentication fails.

Step5: The meter provides information to the master station. The meter encrypts $ID_s$, $ID_c$, $N_s$, $N_c$, and counter initial value $C_i$ with $K_s$, calculates the message authentication code(MAC) of $ID_s$, $ID_c$, $N_s$, $N_c$, $C_i$, $MAC\{ID_s, ID_c, N_s, N_c, C_i\}$, and sends $K_s\{ID_s, ID_c, N_s, N_c, C_i\}$, $MAC\{ID_s, ID_c, N_s, N_c, C_i\}$ to the master station.

Step6: The master station verifies the identity of the meter. The master station verifies the $MAC\{ID_s, ID_c, N_s, N_c, C_i\}$, if the verification is successful, the master station decrypts $N_c'$ and compares it with $N_c$. If it is the same, the access authentication is successful, otherwise the authentication fails. Finally, the master station will record the $C_i$. The specific steps are shown in Figure 2.
### 4.3 Session key updates

In the process of data interaction, if the master key $K_s$ is used as the session key, both sides of the communication need to update the $K_s$ regularly. Frequent replacement of the master key will not only bring burden to the communication, but also increase the probability of the session being cracked. Therefore, in this protocol, the master key $K_s$ is used to encrypt the counter value to update the session key to ensure the authenticity, integrity and confidentiality of the data.

---

**Figure 2 Security access protocol of meter**

**Figure 3 Update of session key**
At the beginning of session, the master station and the meter use $K_s$ to encrypt the current value of the counter, and the ciphertext obtained will be used as the session key $CEK$. The data interactions between the master station and the meter use $CEK$ for protection. After the end of communication, the counter value is increased by 1 to prepare for the next session to update the session key.

5. Security and Performance Analysis of the Proposed Protocol

5.1. Security Analysis of Proposed Protocol

This paper proposes a meter and collector access authentication protocol in which the key is used for information encryption and session key update.

In the access authentication stage, the information of authentication is protected by symmetric key. Even if the attackers receive the message, because there are no key, they can't decrypt or tamper the information. In the first step of interaction, the meter $ID_s$ are transmitted in plaintext, even if the $ID_s$ are tampered, the master station will immediately get $ID_s$ and $ID_s'$ are different and output authentication error, which can effectively prevent man in the middle attack. In the authentication process, the random number in each access authentication will change to resist replay attack. Considering the limitations of the application scenario, this paper does not use the time stamp with high hardware requirements.

In the session key update stage, the proposed protocol updates the session key based on the shared secret (i.e. random initial counter value). In this stage, both meter and master station use the master key to encrypt the counter value, and the ciphertext is obtained as the session key. Even if the attacker obtains the current session key, due to he does not have the master key, he cannot crack the current value of the counter to obtain other session keys and crack other session contents, so the proposed protocol has the forward and backward security.

5.2. Performance Analysis of Proposed Protocol

5.2.1. Comparison of calculation time

| Protocol          | Meter   | Master Station |
|-------------------|---------|----------------|
| Proposed Protocol | $5T_s+T_c$ | $4T_s+2T_c$   |
| Yang$^{[5]}$      | $4T_a$  | $4T_a$         |
| Khan$^{[6]}$      | $6T_h+2T_c$ | $7T_h+2T_c$ |

$T_s$ is the time to complete a symmetric encryption/decryption, $T_a$ is the time to complete an asymmetric encryption/decryption, $T_h$ is the time to complete a hash calculation, and $T_c$ is the time to complete a comparative verification.

As can be seen from Table 1, compared with the protocol proposed by Yang, the protocol proposed in this paper only uses symmetric cipher algorithm with high computing speed and low computing resource consumption, compared with the access protocol proposed by Khan, this protocol establishes a secure transmission channel for subsequent interaction to realize the secure transmission of sensitive key data.

5.2.2. Traffic comparison

| Protocol  | Communication cost |
|-----------|--------------------|
| Proposed Protocol | 3 messages        |
| Yang$^{[5]}$      | 5 messages         |
| Khan$^{[6]}$      | 4 messages         |
It can be seen from Table 2 that the proposed protocol in this paper can complete two-way identity authentication by three times of interaction and establish an encrypted transmission channel, which can effectively reduce the authentication overhead, and realize periodic session key update based on shared secret to ensure the forward and backward security of communication.

### 5.2.3. Comparison of storage capacity

| Protocol   | Meter           | Master Station            |
|------------|-----------------|---------------------------|
| Proposed   | Meter $ID_m$, Master key $K_m$, Master station $ID_m$, Initial value of counter $C_i$ | $<ID-K>$ table of meters, Master station $ID_m$, Initial value of counter $C_i$ |
| Yang[5]    | MAC address of meter, Private key of meter, Master station $ID$ | Private key of master station, MAC address table of meter |
| Khan[6]    | Secret value $x_a$, Meter $ID$, Master station $ID$, Symmetric key $K$ | Secret value $x_a$, Meter $ID$, Master station $ID$, Symmetric key $K$ |

As can be seen from table 3, except the asymmetric encryption proposed by Yang, the storage content of this protocol is slightly different. For the master station, it has strong storage and computing capacity, and it is generally not limited by storage and computing resources. For the meter node, it also has the ability to store key, random value of the counter, device ID and other information. This protocol can achieve two-way authentication and establish a secure encryption channel on the premise of meeting the needs of meter nodes.

### 6. Conclusion

In order to meet the demand of secure access to the master station for the lightweight nodes with limited computing resources in the Power Internet of Things, this paper designs a secure access protocol based on symmetric cryptography algorithm. The proposed protocol only uses the symmetric cipher algorithm with fast operation speed and low resource consumption. While realizing the two-way identity authentication between the meter and the master station, it completes the session key synchronization and update based on the initial value of the random initialization counter to establish a secure transmission channel. Finally, compared with other protocols, the proposed protocol is also effective in security and performance.

### Acknowledgments

This paper was supported by Research on Key Technologies of mobile and Internet security of energy Internet (No. 5700-201955463A-0-0-00)

### Reference:

[1] Zhao J, Huang J, Xiong N. An Effective Exponential-based Trust and Reputation Evaluation System in Wireless Sensor Networks[J]. IEEE Access, 2019,7: 33869-33869.
[2] Zheng Y, Li X, Wang M, et al. Flexible Data Access Control Based on Trust and Reputation in Cloud Computing[J]. IEEE Transactions on Cloud Computing, 2017,(99):1-1
[3] You J, Shangguan J, Zhuang L, et al. An Autonomous Dynamic Trust Management System with Uncertainty Analysis[J]. Knowledge-Based Systems, 2018, 161(DEC.1):101-110.
[4] Fu Ge, Zhou Nian-rong, Wen Hong. The Study of Security Issues for the Industrial Control System Communication Protocols in Smart Grid System[J]. Information Security and Technology, 2014(01):36-38.
[5] Wenbin Fan. Analysis of Security Protection on Industrial Control Protocol [J]. Electronic Science and Technology, 2015, 2(003):334-337.
[6] Zhu Ting Ting. Wireless Security Authentication Protocol Based on Elliptic Curve Signcryption Scheme [J]. Journal of Wuhan University of Technology, 2013, Vol.35 NO.6:145-150.
[7] JIAN Bo, GUO Yonghui, LUO Changyuan. Key Management Protocol for WSN Based on ECC[J]. Computer Engineering, 2010, 36(3):142-144.

[8] Ding Y. Key management scheme for WSN using ECC[J]. Journal of Xidian University, 2008, 35(4):739-742.

[9] Lee S, Bong J, Shin S, et al. A security mechanism of Smart Grid AMI network through smart device mutual authentication[C]// International Conference on Information Networking. IEEE, 2014.

[10] Yang Chaunkai, Jian Yongfeng, Ren Shuangzan, Ding Bin. Power LTE network security access technology based on improved authentication protocol [J]. Electrical Measurement and Instrumentation, 2019, v.56;No.704(03):99-104+110.

[11] Khan, Muhammad Khurram, Alghathbar, etc. Sensors, Vol. 10, Pages 2450-2459: Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'[J]. 2010.