A Secure and Fast Access Protocol for Collecting Terminal in Power Internet of Things based on Symmetric Cryptographic Algorithm

Feng Zhai[1, 2], Yingjie Zhao[1, *], Lingda Kong[1], Xiaojuan Zhang[1], Lin Jiang[1]

[1] China Electric Power Research Institute, 100192 Beijing, China
[2] Tianjin University, 300072 Tianjin, China

Abstract. The development of Power Internet of Things has brought a variety of access requirements for massive collecting terminals. Based on the characteristics of security attributes of Power Internet of Things, this paper proposes a secure access protocol based on symmetric cryptographic algorithm for the large number of collecting terminals with limited manufacturing cost, computing power and storage resources. This protocol only uses the symmetric cryptographic algorithm which has the fast computing speed and low resource consumption, and the protocol can realize two-way identity authentication between the collecting terminal and master station. At the same time, combined with the historical access mechanism, it improves the access efficiency of the collecting terminals, and realizes the safe and fast access of the collecting terminal. Finally, compared with other protocols, the proposed protocol is also effective in security and performance.

1 Introduction

Most of the existing power information systems use physical isolation to ensure the reliability and security of information interaction[1]. The integration of power system and information system will lead to the blurring of the boundary between physical and cyber. With the increasing demand for interaction between grid and users, the Power Internet of Things presents the characteristics of increasing types and numbers of access terminals and expanding coverage. The power system has gradually developed from a relatively isolated industrial control system to a relatively open Power Internet of Things. The instruction, action and state of information system will affect the power physical system deeply.

Cryptography can reconstruct the security boundary by identification and data encryption, it can maintain the security of network information. Cryptography can effectively reduce the risk of illegal access, data theft and tampering through security access and authentication. However, due to the constraints of application scenarios and manufacturing costs, its computing power and storage resources are limited, which cannot meet the requirements of traditional cryptographic algorithms and affect the efficiency of terminal accession. Therefore, combined with the characteristics of limited resources and capabilities of collecting terminals, this paper designs a lightweight Power Internet of Things security access protocol based on symmetric cryptographic algorithm to meet the security access requirements of mass data collecting terminals.

2 Related Work

Some scholars have improved the general internet security protection methods and applied them in power information system. Fu[1] proposed the deployment of industrial firewall, IDS protection equipment and the use of security protocols. According to Modbus protocol, Fan[2] proposes a scheme of applying deep packet detection in firewall. However, these protocols are only improving the traditional protection methods, which are not suitable for the Power Internet of Things with its own characteristics and needs.

Some scholars have designed access protocol based on Elliptic Curve Cryptography (ECC). Zhu[3] uses the trusted certificate agent in ECC signature, which improves the efficiency of device access by reducing the number of interactions, but the protocol has a large time complexity. Jian[4] analyzes the characteristics of sensor networks, and proposes a key agreement protocol based on ECC algorithm. It improves the computing speed by shortening the key length, but reducing the key length reduces the security of the protocol.

Some scholars solve the security access problem of power grid terminal by calling the third part service. Lee[5] designed a two-way authentication mechanism for smart grid devices based on Public Key Infrastructure (PKI), which reduced the interactions in the authentication process. Yang[6] aimed at the access scenario of massive transmission line monitoring terminals, based on PKI,

* Corresponding author: zhaoyj@epri.sgcc.com.cn

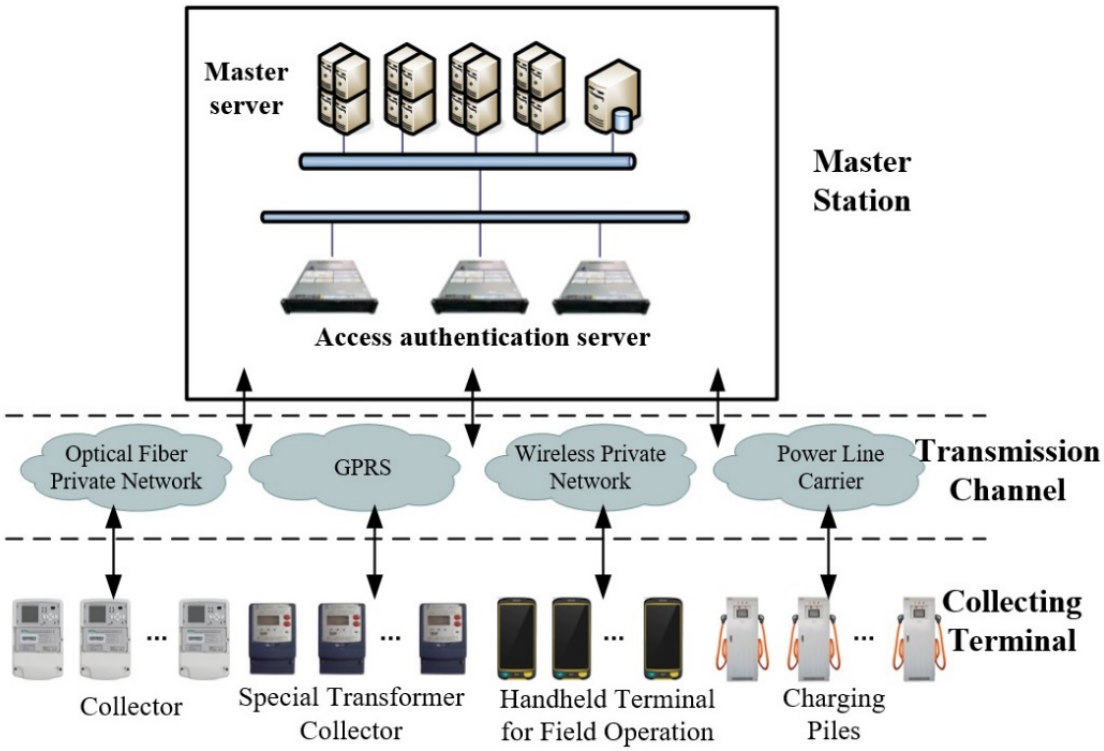

Fig. 1. Power Information Collection Network

completed the authentication of monitoring terminal and master station server, and realized the key update through asymmetric cryptographic algorithm. Due to calling the third part service, these protocols increase the communication overhead of the system. The asymmetric cryptographic algorithm involved in PKI requires higher computing ability of the terminals.

In addition, some scholars use other cryptographic algorithms to achieve secure access authentication. Ren[7] proposes a key agreement protocol based on the q-ABDHE mathematical difficulty assumption and the deterministic BDH assumption, using the idea of MTI protocol. The protocol requires more storage for the central node, and there is no two-way identity authentication in it. Das[8] uses a combination of hash and symmetric cryptographic algorithm to complete the security access authentication of the master station to the terminal, but it ignores the two-way identity authentication, which has the risk of fake master station attack.

These studies use different methods, including improving the general security protection methods, improving ECC algorithm and calling third-party services. However, they seldom consider the limitations of terminal manufacturing cost, computing power and storage capacity. Therefore, their adaptability to the power Internet of things is limited. This paper aiming at the security and fast access requirements of lightweight collecting terminal, designs a lightweight Power Internet of Things security access protocol based on symmetric cryptographic algorithm, and realizes the security and fast access of collecting terminals in Power Internet of Things.

3 Characteristics of Power Internet of Things

With the application of advanced information technologies in the power grid, the Cyber Power Physical System is gradually formed. Figure 1 shows the structure of power information collection network. Information technology enhances the interaction between power grid and users. The power grid can not only meet the personalized needs of customers, but also guide users habits to reduce the load fluctuation. Through meteorological big data prediction and distributed control system, information technologies can improve the power grid ability to absorb clean energy. By deploying the sensor terminals to collect the load and equipment status, artificial intelligence technology can be used to assist power grid dispatching and optimize the operation status of power grid.

Due to the combination of power physical system and its unique business, information system presents different characteristics. Different from the general Internet, most of the devices in the power grid adopt the method of embedded security module, which determines that their computing power, memory resources and data transmission speed are limited. The requirement of real-time data of power grid information system changes with the demand of business system, and once the equipment is put into operation, it is difficult to replace or upgrade them offline.

According to the above analysis, consedering the differences between the power information system and the general internet, it is necessary to study the secure and fast access protocol, which is suitable for the Power

Internet of Things, so as to meet the secure and fast access requirements of the collecting terminals.

4 A Secure and Fast Access Protocol based on Symmetric Cryptographic Algorithm

This paper designs a secure and fast access protocol based on symmetric cryptographic algorithm for the Power Internet of things to achieve two-way identity authentication between the collecting terminals and the master station, it also improves the access efficiency of the collecting terminals based on the historical access mechanism.

4.1 System Initialization

The security chip used to store the key is embedded in the collection terminal. The collecting terminal completes the key infusion and entries the corresponding master station information before operation. The master station deployed the security device to store the key, and also stored the <Identity-Key> table of the collecting terminals.

4.2 Terminal Access Authentication

Step 1: The terminal sends the access authentication request to the master station. The terminal generates random number N_s, encrypts terminal ID_s, random number N_s and terminal Media Access Control Address (MAC_s) with symmetric key K_s, and sends K_s {ID_s, N_s, MAC_s} and ID_s to the master station.

Step 2: The master station verifies the identity of the terminal preliminarily. According to ID_s, the master station searches the corresponding key K_s in the <Identity-Key> table and decrypts it, records the terminal's MAC_s in the master station's MAC list, and compares whether the ID_s' and ID_s are the same. If they are the same, proceed to the next step, otherwise the authentication fails.

Step 3: The master station verifies the identity to the terminal. The master station generates the random number N_c, encrypts the master station ID_c and the random number N_s, N_c with the symmetric key K_s, and sends K_s {ID_c, N_s, N_c} to the terminal.

Step 4: The collecting terminal verifies the identity of the master station. The collecting terminal decrypts the massage and verifies the consistency of the decrypted N_s' and N_s, the ID_c' and ID_c. If they are the same, go to the next step, otherwise the authentication fails.

Step 5: The terminal verifies the identity to the master station. The terminal uses the symmetric key K_s to encrypt ID_s, ID_c, N_s, N_c, get K_s {ID_s, ID_c, N_s, N_c}, and send it to the master station.

Step 6: The master station verifies the identity of the terminal. The master station decrypts K_s{ID_s, ID_c, N_s, N_c}, obtains N_c' and compares it with N_c. Finally, the master station classifies MACs into whitelist or blacklist according to the results. Figure 2 shows the process of the access protocol.

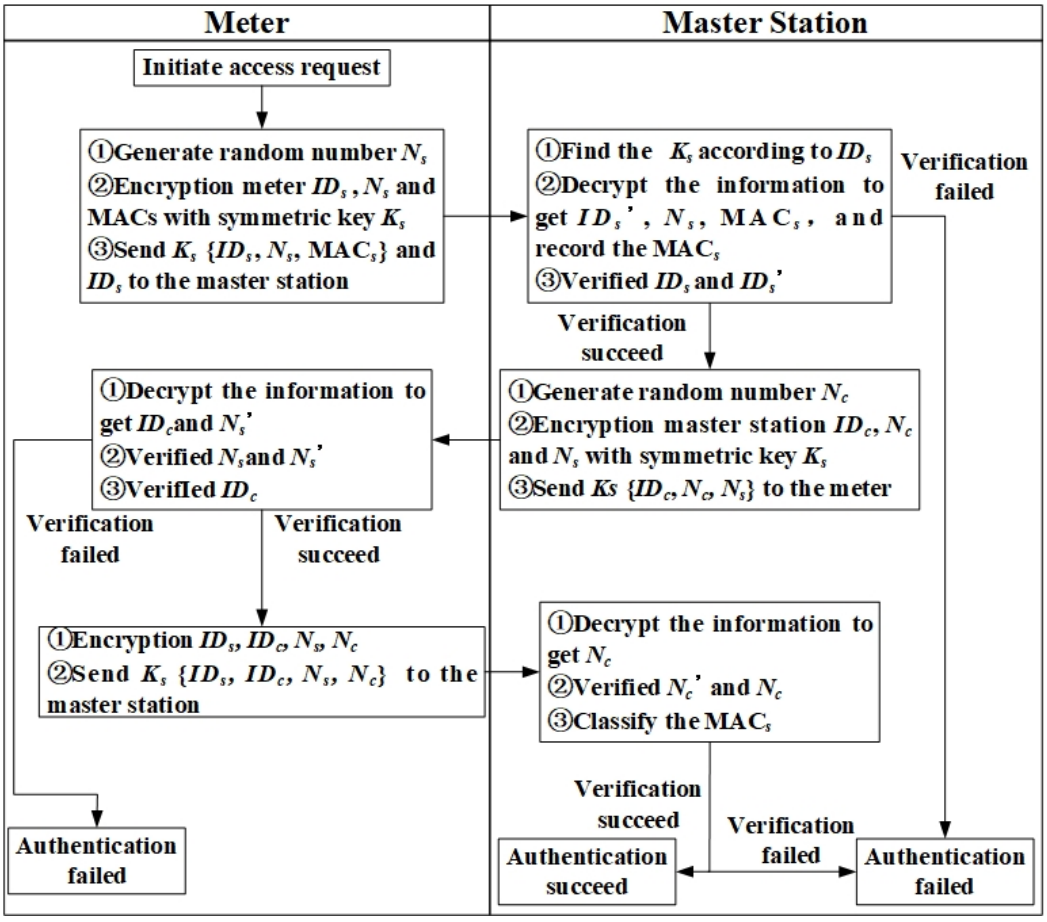

Fig. 2. Security Access Protocol of Collecting Terminal

4.3 Historical Access Mechanism based on MAC of Collecting Terminal

When the collecting terminal access, only the IP address will change, and the MAC*s* of the terminal won't change. Therefore, this paper uses the historical access mechanism to improve the access efficiency of the collecting terminals. The MAC list in the master station is divided into whitelist and blacklist. For the terminals that have successfully accessed for many times will be entered to the whitelist, and that have failed to authenticate for many times will be entered into the blacklist. When a terminal is accessed, the master stations first search and compare the MAC*s* in the MAC list, gives priority to the terminals in the whitelist, refuses the access request to the terminals in the blacklist, and transfers the non-existent terminals to the access process for authentication, and enters their MAC*s* into the whitelist or the blacklist according to the results. The historical access mechanism can effectively improve the access efficiency of terminals, prevent the Denial of Service attack caused by malicious terminal access requests.

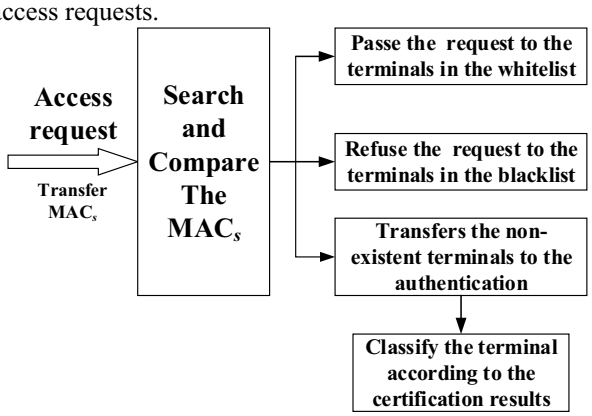

Fig. 3. Historical Access Mechanism

5 Security and Performance Analysis

5.1 Security Analysis of Access Protocol

In the access authentication protocol proposed in this paper, the collecting terminal initialization and key synchronization are completed before the terminal runs, and the master symmetric key is stored and used in the security chip. Before the access, the protocol adopts the historical access mechanism. It compares the terminal MACs in the MAC list, and classifies the access collecting terminals to improve the access efficiency.

In the access authentication, the information of authentication is protected by symmetric key. Even if the attacker receives the message, due to don't have the key, they can't decrypt it or tamper the information. In the first step of interaction, although the collecting terminal IDs are transmitted in plaintext, even if the IDs are tampered with, the master station will immediately get IDs and IDs' are different and output authentication failed, which can effectively prevent the middle attack.

In the authentication process, both sides of the interaction complete the challenge-response based on random number, and it will change in each access authentication. Considering the limitations of the application scenario, the proposed protocol doesn't use the time stamp with high hardware requirements to reduce the cost of the terminal, resist the replay attack and complete the two-way identity authentication.

The whole access authentication and information encryption is based on the symmetric cryptographic algorithm. The collecting terminal only needs to execute the symmetric cryptographic algorithm, which has the advantages of fast computing speed and less resource consumption. It reduces the hardware requirements for the collecting terminals, the complexity of equipment access authentication, and improves the adaptability of this protocol in the Power Internet of Things.

5.2 Performance Analysis of Access Protocol

5.2.1 Comparison of calculation time

Table 1 Consumption time of access authentication for each protocol

Protocol	Collecting Terminal	Master Station
Proposed Protocol	3Ts+Tc	3Ts+2Tc
Yang[6]	4Ta	4Ta
Das [8]	4Th+Ts	2Th+2Ts+2Tc

Ts is the time to complete a symmetric encryption/decryption, Ta is the time to complete an asymmetric encryption/decryption, Th is the time to complete a hash calculation, and TC is the time to complete a comparative verification.

As we can see from Table 1, compared with the Yang protocol, the proposed protocol only uses symmetric cryptographic algorithm with high computing speed and low computing resource consumption. Compared with Das protocol, the proposed protocol increases part of the computational cost, but realizes the two-way authentication between the collecting terminal and the master station to prevent the attack of fake master station.

5.2.2 Traffic comparison

Table 2 Communication cost of each protocol

Protocol	Communication cost
Proposed Protocol	3 messages
Yang[6]	5 messages
Das [8]	2 messages

It can be seen from Table 2 that in the authentication protocol proposed in this paper, the two-way authentication can be completed after three times of

interaction between the collecting terminal and the master station. The protocol proposed in this paper effectively reduces the communication times.

5.2.3 Comparison of storage capacity

Table 3 Storage content required by access authentication protocol

Protocol	Collecting Terminal	Master Station
Proposed Protocol	Collecting Terminal ID_s, Master key K_s, Master station ID_c, Media Access Control Address (MAC_s)	<ID-K_s> table, Master station ID_c, Media Access Control Address (MAC_s)
Yang[6]	collecting terminal MAC*s*, Private key of collecting terminal, Master station *ID*	Private key of master station, MAC*s* address table of collecting terminal
Das [8]	Secret value x_a, collecting terminal *ID*, Master station *ID*, Symmetric key *K*, Random number *y*	Secret value x_a and x_s, <ID-K_s> table

As can be seen from Table 3, except the protocol proposed by Yang, the storage content of other protocols is almost same. For the master station, it has strong storage and computing capacity, and it is generally not limited by storage and computing resources. For the collecting node, it also has the ability to store key, random value, device ID and other information.

6 Conclusion

In order to meet the security requirements of the limited computing resource terminal access to the master station in the Power Internet of Things, this paper designs a secure access protocol based on symmetric cryptographic algorithm. This protocol only uses the symmetric cryptographic algorithm with fast operation speed and low resource consumption, which can realize the two-way identity authentication between the collecting terminal and the master station. At the same time, it uses the historical access mechanism to classify the access collection terminals, so as to improve the access efficiency. 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).

References

1. Fu, G., Zhou, N.R, Wen, H. (2014) The Study of Security Issues for the Industrial Control System Communication Protocols in Smart Grid System. Info. Sec. & Tec., 01: 36-38.
2. Fan, W.B. (2015) Analysis of Security Protection on Industrial Control Protocol. Elec. Sci. & Tec., 003: 334-337.
3. Zhu, T.T. J. (2013) Wireless Security Authentication Protocol Based on Elliptic Curve Signcryption Scheme. Wuhan. Uni. Tec., 35: 154-150.
4. Jian, B., Guo, Y.H., Luo, C.Y. (2010) Key Management Protocol for WSN Based on ECC. Comp. Eng., 36: 142-144.
5. Lee, S., Bong, J., Shin, S., Shin, Y. (2014) A security mechanism of Smart Grid AMI network through smart device mutual authentication. In: International Conference on Information Networking. IEEE. Phuket. 592-595.
6. Yang, C.K., Jian, Y.F., Ren, S.Z., Ding, B. (2019) Power LTE network security access technology based on improved authentication protocol. Elec. Meas. & Instr., 56: 99-104+110.
7. Ren, Y. J., Wang, J.D., Xu, D.Z., Zhuang, Y. (2010) Enhanced Identity-Based Authenticated Key Agreement Protocols in the Standard Model. J. Comp. Res. & Dev., 47: 1604-1610.
8. Das, A.K., Sharma, P., Chatterjee, S., Sing, J.K. (2012) A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. J. Net. & Comp. Apps., 35: 1646-1656.