Research on Security Mechanism of Service Interoperability Based on Power Grid Computer System

Yuling Zhang¹, Jijun Wang², Wencheng Liu³, ⁴* and Ting Wang³, ⁴

¹Wuxi power supply branch of State Grid Jiangsu Electric Power Co., Ltd., Jiangsu, China
²Jiangsu Electric Power Information Technology Co., Ltd., Jiangsu, China
³Shenyang Institute of Automation, Chinese Academy of Sciences, Liaoning, China
⁴Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences

*Corresponding author e-mail: liuwencheng@njust.edu.cn

Abstract. With the gradual development of the power grid computer system, more and more intelligent power equipment is connected to the service system, and the security of service interoperability in the computer system is gradually concerned. This paper evaluates the security problems of power grid computer system, combines PKI system with OPC UA protocol, and uses data transmission technologies such as digital digest and symmetric encryption to ensure the security of data transmission.

Keywords: Power Grid; Service Interoperability; Security; OPC UA

1. Introduction

With the development of power grid industry towards intelligence, more and more attention has been paid to its security. In the early stage of smart grid system development, only considering its functional requirements, ignoring security risks, lack of authentication protection, encryption protection and integrity protection and other security mechanisms.

Aiming at the security risk of service interoperability in power grid industry, this paper improves the security mechanism of OPC UA, integrates information security and OPC UA into power grid industry, and establishes security architecture of OPC UA based on power grid.

2. Related Work

2.1. OPC UA

2.1.1. Network level of OPC UA
OPC UA defines standard APIs for data collection, events and alerts, historical data, and support metadata to provide semantic description support [1]. As shown in the figure 2.1, examples of OPC UA application at different network levels are given. In the underlying device layer, OPC UA server can not only run on the controller of the device, but also connect with the controller of the device through the underlying network to obtain the data of the device.
In the operation network layer above the bottom layer, OPC UA applications may be used as both clients and servers. The top layer is the enterprise network. The OPC UA client integrated in the ERP system can obtain the information of the equipment used at the bottom of the factory. The company's network layer allows remote access to OPC UA servers over the Internet for service or maintenance work.

![Network level of OPC UA](image)

**Figure 1. Network level of OPC UA**

### 2.1.2. OPC UA security architecture

The security architecture of OPC UA is shown in the figure 2.2. The security architecture is defined, and each layer has specific responsibilities.

The bottom layer is the transport layer, whose responsible is the security of receiving and sending data through socket connection. The middle layer is the communication layer, which needs to provide a security channel for the upper session. The security channel ensures the confidentiality and integrity of the application. The top layer is the application layer, which is used to transfer the factory information, settings, instructions and real-time related data from the device in a session between the client and the server. The security means used in session part include user authentication and authorization, product authentication and authorization[2].
2.2. Safety Risk Assessment of Power Industry

More and more different types of smart devices are needed to access the intranet of power enterprises and exchange data with intranet application systems. The emergence and popularity of smart terminals has convenience to users, but it also has brought many potential threats, such as illegal tampering and illegal access of information, using the operating system to modify relevant terminal information, and destroying the system through viruses and malicious code [3]. The access of intelligent devices brings new security problems to the security of enterprise intranet information, which is mainly reflected in the security of terminal equipment, transmission channel and application system[4].

The security risk of power terminal equipment is the uncertainty of equipment manufacturers, and the terminal equipment lacks encryption mechanism for important data files;

The security of transmission channel. In the process of data exchange with the intranet, the data transmission channel may still face the risk of data interception or tampering, and the transmission channel will be destroyed.

The security of application system. Intelligent terminal equipment is normally connected to the power enterprise intranet, as a trusted user within the enterprise. If the identity of the successful access terminal is illegal, it will increase the hidden danger of uncontrollable security in the enterprise intranet, which will lead to the illegal invasion of the intranet application system of the power enterprise and the theft of important information.

3. OPC UA Security Mechanism in Power Industry

3.1. Security Architecture

The security architecture proposed in this paper constructs a secure channel in the client and server of OPC UA, and introduces PKI system, digital signature and digital digest technology. As shown in the figure 3.1, the connection between OPC UA client and server is established on the basis of trusted certificate. The management of certificate is PKI system. The communication after connection uses digital signature and digital digest symmetric encryption for data transmission to ensure the integrity of information and not be tampered with.

Figure 2. OPC UA security architecture
3.2. Secure Connection Establishment

In this paper, the establishment of security connection is the establishment of security trust between entity objects. Entity objects include OPC UA client and OPC UA server.

(1) Certificate application

For different application scenarios, both OPC UA client and OPC UA server need to apply for certificates. This paper describes them as entity objects.

The steps for entity objects to apply certificates are as follows in the figure 3.3. RA is the Registration service RA, which is the basic starting service of PKI service. CA service is the core executive organization of PKI and the main component of PKI.

There are two kinds of certificates applied by entity objects in this paper. One is the application instance Certificate in OPC UA architecture specification, which identifies the opcua program instance running on the host. The other is the software certificate in OPC UA architecture specification, which identifies a specific version of OPC UA products. Through the information exchange when establishing the connection, both programs know whether they can communicate with each other in an appropriate way.

(2) Establishment process of secure communication channel for OPC UA client server

Firstly, the OPC UA client sends a request to the OPC UA server to obtain the server information and the request is not secure. The server feeds back the application instance certificate to the client. The client initiates the server certificate verification request to the authentication service of PKI system.

If the verification is passed, the client will make a security request, that is, sign and encrypt the request information. The certificate private key of CA client is used for signature, and the public key of server certificate is used for encryption. After receiving the request, the server first verifies the...
validity of the client certificate to the PKI verification service, decrypts the client certificate with the server's private key, and verifies the signature of the message with the initiator's public key. After the verification and decryption is passed, the client will respond to the information and connect the secure channel to complete the establishment.

Finally, a secure session is established on the basis of the secure channel established in the previous step. After the client sends a request, the server will provide its own software certificate to respond to the request. In addition, it may prove the ownership of the certificate through the challenge response test. In addition, the system will generate a valid session ID for each session to prevent replay attacks. In order to realize the dialogue between applications, the client must send a request to activate the session. When the server receives the request, it will verify the client's software certificate and entity credentials, including the user name and password or the entity's certificate.

3.3. Data Security Transmission
Data transmission is the core part of the security mechanism of service interoperability. Data transmission is based on the security channel. The establishment process of connection security channel has been described in the previous section. Data security transmission relies on symmetric encryption and digital digest technology.

(1) Symmetric encryption
AES encryption algorithm is used in symmetric encryption algorithm. The key of symmetric encryption algorithm is that the receiver determines the key in the process of establishing a secure channel, and encrypts and transmits it to the sender with the certificate public key of the initiator. The sender decrypts the private key to obtain the symmetric key of data transmission, so as to ensure the security of symmetric key transmission of data transmission [5].

AES-128 is recommended in this paper, that is, the key length is 128 bits and the number of encryption rounds is 10. At the beginning, we need to perform round key addition operation for plaintext, and then do 10 rounds of encryption. The round functions of the first round to the ninth round of encryption are the same and the order is the same, which are byte substitution, row displacement, column mixing and round key addition. Round 10 is different and does not perform column mixing. The decryption process of AES is still 10 rounds, and each round of operation is the reverse operation of encryption operation.

(2) Digital digest
Digital digest is to change any length message into a fixed length short message. The purpose of using digital digest in this paper is to verify the integrity of the transmission information and not to be tampered with. In addition, for the scenario with large amount of data, the security transmission process is more efficient and time-consuming is reduced.

The plaintext uses hash algorithm to calculate plaintext digest, and then the sender uses the sender's private key to digitally sign the digest, and then encrypts the original text and digital signature with AES key to obtain ciphertext and transmit the ciphertext to the receiver. After receiving the ciphertext, the receiver uses AES key to decrypt the ciphertext, and obtains the digital signature and the original text respectively. Then, the sender's public key is used to decrypt the digital signature to obtain digest 1. Then hash algorithm is used to calculate the summary of the original text, and the digest2 is obtained. Comparing the content of digest 1 and digest 2, if the content is consistent, the original text is not tampered with and trusted, so the data security transmission is completed.

4. Safety Analysis
The OPC UA security mechanism designed in this paper meets the requirements of connection trustworthiness, data integrity, confidentiality and availability.

(1) Connection trustworthiness
The PKI system designed in this paper is the core of establishing secure connection. The security connection between OPC UA client and server depends on the trust of both sides' certificates, and the premise of certificate trust is the CA trustworthiness of PKI system, so the security of PKI system is
very important. Therefore, in practical application, PKI system should be installed and deployed in the security server to ensure that the security of PKI system is not attacked.

(2) Data integrity
Data integrity is to confirm that the data has not been modified. In the process of data communication, the security mechanism designed in this paper uses the digital digest technology to decrypt the digital signature to obtain the original abstract, and decrypt the ciphertext by AES algorithm, and calculate the digest by hash function to compare the consistency of the two digests, so as to evaluate whether the data has been tampered and modified, and ensure the integrity of the data.

(3) Confidentiality
In this paper, on the one hand, CA certificate is used to realize the establishment of secure channel, on the other hand, AES encryption technology is used. The key of AES encryption technology is how to inform the other party. After establishing a secure connection channel by using digital certificate, the sender automatically generates symmetric key, and then encrypts the key by using the private key of the sender's certificate to the receiver, the receiver uses the public key of the sender's certificate to decrypt, which ensures the encryption of the key transmission. At the same time, the digital digest technology is used to increase the integrity verification mechanism of the key transmission.

(4) Availability
The application scenarios of OPC UA in the power industry include data acquisition, and the release of northward cloud platform. It needs high real-time performance. In this paper, considering the requirement of real-time, the symmetric encryption technology based on the establishment of secure channel is adopted for data transmission encryption technology, which reduces the calculation amount of encryption. At the same time, asymmetric encryption of digital digest is adopted to enhance the security of data. Through the practical application test, the time difference between the data delay of increasing security mechanism and OPC UA without security mechanism is between 10ms ~ 15ms, which meets the real-time requirements of power industry.

5. Conclusion
In this paper, aiming at the safety risk assessment of OPC UA in power industry, the security mechanism architecture of OPC UA in power industry is designed. Combining PKI system with OPC UA protocol, a complete security mechanism from secure connection to data communication is constructed. In the process of data communication, the technology of digital digest and symmetric encryption is proposed. Through the analysis of security test, the trust, integrity, confidentiality and availability of information security are satisfied.

References
[1] Haoyu Yu, Dong Yu, Yi Hu, Chuting Wang. Research On CNC Machine Tool Monitoring System Based On OPC UA [A].
[2] Northeast University, China Society of Automation Information Physical System Control and Decision-Making Professional Committee. Proceedings Of The 31st Chinese Conference On Control And Decision-Making (3) [C]. Control and Decision-Making Committee of Information Physics System, Northeast University, China Automation Society, 2019:5.
[3] Mank, Lightner, Damma Guohua. OPC Unified Architecture [M]. China Machine Press, 2012.
[4] SHI Shuhong, Wang Lei, Zheng Shiqiang, LV Jingwei, Zhang Qian. Research on Multiple Security Authentication Schemes for Mobile Applications of Power Trading Platforms [A]. Auckland University of Technology, Hong Kong Society of Mechanical Engineers (HKSME).Proceedings of 2019 4th Asia Conference on Power and Electrical Engineering (ACPEE 2019) [C]. Auckland University of Technology, Hong Kong Society Of Mechanical Engineers (HKSME): Chengdu Shylock Education Consulting Co., Ltd, 2019:6.
[5] Sun Hung-Keung. Research and Implementation of Security Access System for Power Mobile Terminal.