Implementation and research of a substation command interaction method using third party validation

Implementation and research of a substation command interaction method using third party validation

Sun Shucai[1,2], Zhu Chenpeng[1,2] and Xie Yehua[1,2]

1 NARI Group Corporation/ State Grid Electric Power Research Institute, Nanjing, CHN
2 NARI Technology Development Co.,Ltd, Nanjing, CHN
E-mail: sunshucai@sgepri.sgcc.com.cn

Abstract. This paper describes a method to improve the security of control signal transmission in substation by introducing third party authentication and applying encryption technology. We can use asymmetric encryption technology to ensure the safety of data transmission process. A third party authentication device is introduced to verify the rights and identities of both sides of the command and prevent the interception and tampering of command information. Use dynamic key and authorization expiration system to further protect control security. Finally, the character code is checked by the command and the error data is filtered effectively. This method can effectively prevent signals from being truncated or tampered and ensure the security of data. Restricting the operation crowd, isolating illegal users, protecting information security, greatly improve the information security of substation control process.

1. Background technology

1.1. SSL Encryption technology

Secure Socket Layer enables communication between Client and server not to be eavesdropped by an attacker, and always authenticates the server and the user optionally. Secure Socket Layer has completed encryption algorithm, communication key negotiation and server authentication before application layer communication. The data transmitted by the application layer is encrypted to ensure the privacy of communication. The data transmitted by the application layer is encrypted to ensure the privacy of communication[1].

1.2. Asymmetric encryption algorithm

Asymmetric encryption algorithm, also known as "public key encryption algorithm", requires two keys: public key and private key. The public key and the private key are a pair. The data is encrypted with the public key and can be decrypted only with the corresponding private key. Encrypting data with a private key can only be decrypted with the corresponding public key. Encryption and decryption use two different keys. This algorithm is called asymmetric encryption algorithm.

The strength and security of the algorithm depend on the algorithm and key. The speed of encryption and decryption is not as fast as that of symmetric algorithm. But there is only one key in the symmetric algorithm. Decryption needs to know the key first, to guarantee the security. To ensure the security of the key, asymmetric encryption algorithm has two kinds of keys, one of which is public [2].

1.3. Hash algorithm

Hashing algorithm can generate fixed length output for different length of input messages. Hash algorithm is a one-way encryption algorithm, which can not be decrypted by encrypted text to get plaintext. Even for minor changes in plaintext, the same hash operation will get completely different results. Based on this characteristic, hash algorithm is usually used to verify the integrity of information[3].

2. System Deployment and Object Definition

The method described in this paper is to introduce third party authentication and apply encryption technology. This method can improve the security of signal transmission in substation, prevent signal interception or tampering, ensure the security of data, limit the operation crowd, isolate illegal users, protect information security and other functions[4].

The simple system deployment structure is as figure 1:

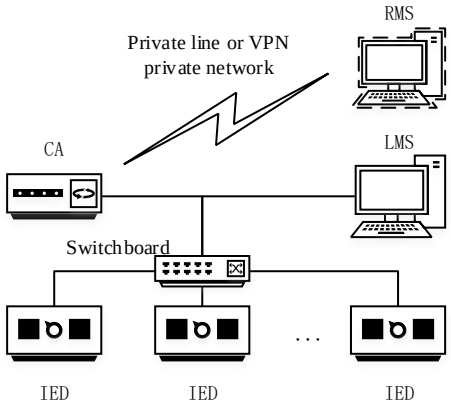

Figure 1. Simple schematic diagram of system deployment structure.

2.1. Authorized authentication device（hereinafter referred to as CA）

The device is a trusted third-party verification device used in this method. As the guarantee of data security and the safe transfer of control commands, it has the following main functions:

- The function of acquiring authentication authority through smart card or digital certificate.
- The function of issuing, managing and authenticating data certificates.
- The function of SSL encryption communication.
- The function of checking information integrity.
- The function of recording and auditing the authorized information.

2.2. Local monitoring system（hereinafter referred to as LMS）

LMS is the local management system for monitoring and operating IED(generally referred to as SCADA systems, this article only emphasizes its local control role),as the control command initiator in this method[5]. Compared with the traditional system, it needs to be extended to improve its security, and has the function of processing encrypted information, as follows:

- Upgrade the authentication mechanism to bind it to the authorized authentication device, and use the digital security certificate to improve the security of the account.
- Upgrade the data communication program, so that it can use SSL encryption mechanism to interact with the authorized authentication device.
- Calculate the hash code of information and verify the integrity of information.

2.3. Remote monitoring system（hereinafter referred to as RMS）

The system is a remote management system for monitoring and operating IEDs (generally referred to as the dispatching master station system), which interacts with LMS through dedicated lines or private networks. In this method, the command of RMS is directly interacted with CA, and is the initiator of the remote control command[6].

2.4. Intelligent equipment（hereinafter referred to as IED）

The device is the smart unit that handles the execution of the control command in this method. It is the receiver of the control command. As the receiver and processor of the final information, it is a very important part of the whole control process[7]. The device has the following functions:

- Receive, store and forward hash feature codes sent by LMS.
- Upgrade the data communication program, so that it can use SSL encryption mechanism to interact with the authorized authentication device.
- Calculate the hash code of information and verify the integrity of information.

3. Identity Authentication Mechanism

3.1. Authentication method based on CA certificate

In order to ensure its security from intrusion, CA, as the default trusted device of this method, is developed based on embedded system[8] and only runs the necessary functions. The digital certificate is solidified on the hardware, which is used for external authentication and is unique.

For local control, a list of trusted smart cards is set up to obtain the authentication key of the device authorization. Local operation needs to provide a smart card before CA can grant remote control operation privileges, which can effectively control the scope of local operation terminals and personnel.

For remote control, a list of trusted devices is established, corresponding digital certificates are stored to verify the identity, and reliable data channels are used to transmit authentication information first[9]. After CA authenticates the identity reliably, it opens remote control privileges and effectively limits the scope of remote control terminal.

3.2. Authentication method based on LMS certificate

LMS itself has a user authentication mechanism, and its control operation authority is granted by CA. LMS submits authentication information to CA before issuing an operation instruction. CA verifies the identity of LMS by verifying the digital signature according to the recorded information. Identity trust is temporary. After more than one operation cycle, CA will reclaim control authority and issue new digital certificates.

3.3. Authentication method based on RMS certificate

RMS itself is secure and has user authentication mechanism. Control rights within the substation are granted by CA. RMS actively exchanges digital certificates with CA before issuing an operation instruction. After cross-validation, CA opens control rights to RMS. Control rights are temporary, and beyond the agreed time, CA will reclaim control rights and require RMS to update digital certificates.

3.4. Authentication method based on IED certificate

IED can update its own digital certificates according to needs. The identity of IED is managed by CA, which establishes a library of intelligent devices, records equipment information, and is responsible for requesting and verifying digital certificates.

4. Interaction Process

This article takes the local control process as an example, as follows:

The use of sections to divide the text of the paper is optional and left as a decision for the author. Where the author wishes to divide the paper into sections the formatting shown in figure 2 should be used.

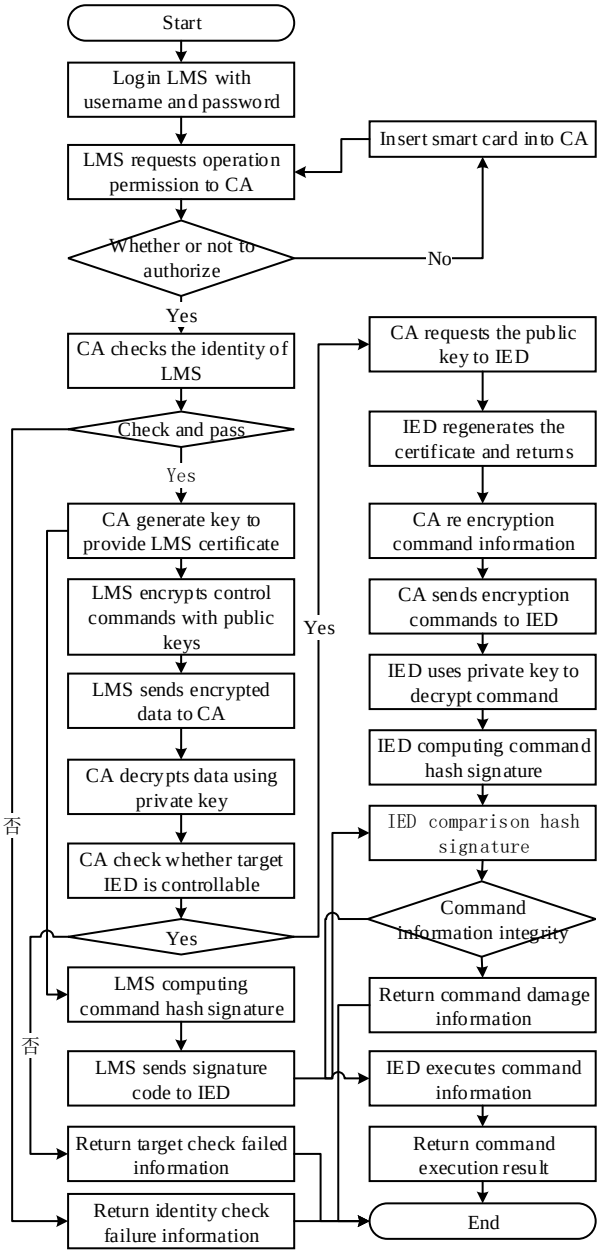

Figure 2. This method controls the flow chart of interaction process.

4.1. Initiation of control instructions

4.1.1. Get CA permission. The operator first needs to hold smart card and use smart card to get the access right of CA.

4.1.2. Sign in LMS. Use user name and password to log on to LMS. The account used needs to have control authority. operator first needs to hold smart card and use smart card to get the access right of CA.

4.1.3. Application control operation authority. The operator operates on the LMS, and the program automatically sends the request to CA. CA verifies the identity information of the monitoring device, returns a one-time public key when the verification passes, and terminates the control process if the verification fails[10].

4.1.4. Encryption control command. The LMS control program encrypts the control command using the received public key, and generates hash signatures for the control command for integrity checking. LMS submits the encrypted control command to CA and sends the hash feature code to the IED that needs to be operated.f

4.2. Transfer of control instructions

4.2.1. Declassified control command. After receiving the encrypted control command, CA uses its own private key to decrypt.

4.2.2. Check device control authority. CA checks whether the target IED is in the control range according to the control command.

4.2.3. Get the target IED public key. According to the parsed control command, the CA sends a command to update the certificate to the target IED. The IED regenerates the certificate and passes the public key to the CA.

4.2.4. Re-encrypt control command. CA encrypts the control command with the public key obtained and sends the encrypted data to the target IED.

4.3. Control command execution

4.3.1. Declassified control command. IED uses private key to decrypt control commands transmitted by CA.

4.3.2. Check control command. IED calculates the hash signature of the control command and compares it with the hash signature sent by LMS to verify the integrity of the command.

4.3.3. Execution control command. IED performs operations according to the contents of the command.

4.3.4. Re-encrypt control command. CA encrypts the control command with the public key obtained and sends the encrypted data to the target IED.

5. Examples

The following example is illustrated by a simple remote control closing process.

- Controller logs in LMS system with username and password, chooses the equipment object to be controlled, and issues remote control closing command.
- The LMS system detects remote operation and starts operation permission detection. The CA verifies the validity of the smart card or digital certificate. CA reads the certificate data, obtains the detailed information through the system solidified decryption key, carries on the authorization comparison user name, the password, the smart card number and so on information. These information agree that the identity of the operator is legal and verified[11]. LMS requests a communication certificate from CA, which detects a request initiated by LMS and randomly generates a set of asymmetric keys such as figure 3 showing the following key information:

```
m1 =
130ebebd67b16a9ab2c53a437badbf8f01a80c750095a7fcfe95742c3d5
ed1abb318babc5cb5d9350fee4da65ee074f65e1758117e6945f0fcfc81
37528053ce9d1da8618890dee24e5e0bf8c87795bb1d09eddd544640824
ee0dd0ea9fd908d27b0f8a1ae5c37f3647fbf2f5795500ad76c195b3387
d0458a8f51b701472301
e1 = 10001
d1 =
12e8da920d4599458e84ec5ef1656161807f427d05eb79182b7418259d6
f6c14364d1f5caf9130c8d9d9d6ea71d1bdbc87781a46a16bcb9e672814
fed3b9c96ddffe0a1b0955ae68055c8f92fef518a04fc32a2ea8390e617
cc5556a251f9ae9eee70a32e579cb3e9f298848a9b3aaf634f5930ffbf7
4473f7cb6c0cefee1751
```

Figure 3. Schematic key information.

- After LMS receives the key, it begins to transmit data. LMS generates command plaintext based on operation, assuming that the plaintext P1 is as table 1:

Table 1. Motioned remote command.

01	01	01
Destination IED address	Target remote control outlet	The remote control type is closing

Encrypted ciphertext *s1*as figure 4

```
011c74f981f6c6697f22b9d6fabad9cea0d7e4f6fdd05630e1beff1da07
0bcd85cd2872ed30c414ffc0c7f7e3587c3e2afc53b0a278fdb9cb1f6e1
f64a0e052695d1252bb67cfb3ced31e13650cd96cad54b182a48a623af1
2117cf603cf274554b207b2c03048ff5681003e9136c25b74729377a9f2
ee877cc45cd0c4ebd9e9
```

Figure 4. Implied ciphertext s1.

Hashing feature codes *l1* are obtained through hash feature algorithm (such as figure 5).

```
21ef05aed5af92469a50b35623d52101
```

Figure 5. Schematic hash feature code.

Where S1 is sent to CA, and L1 is sent to target IED.

- CA receives the ciphertext S1 sent by LMS, decrypts the ciphertext using D1 and e1, and queries the valid IED table of the local record after obtaining the target IED address[12]. If it is valid, it is considered controllable. If it is invalid, it returns the failure information of the target check.
- After the CA determines the controllability, it requests the encryption key to the target IED, the IED generates a temporary certificate, and feeds back the new *m2* and *e2* to the CA. The CA re-encrypts the plaintext and passes the ciphertext *s2* to the IED.
- As the figure 6 shows, IED decrypts the ciphertext *s2* using the reserved *d2* and *e2*, calculates the hash signature *l2* of the decrypted plaintext *p2*, and compares it with the previously received signature *l1*. The same result means that the command information is correct and can be executed. If the result is different, the command is considered damaged and the order is re-issued.

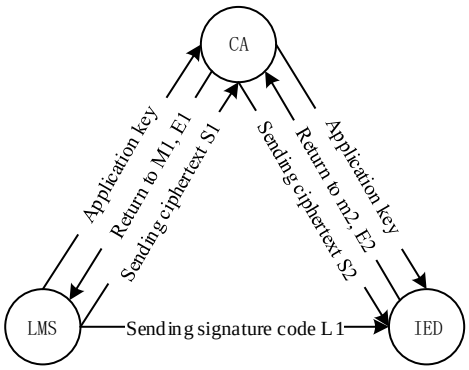

Figure 6. The data exchange process of this example.

6. Conclusion

The method described in this paper can effectively control the control rights and scope of IED equipment, prevent command information from being intercepted and tampered with in the interactive process, verify the integrity of command information, prevent illegal users from gaining operational authority, prevent the execution of wrong commands, and greatly improve the information security of substation control process, especially in unreliable network environment. This method is not restricted to substations, and other field contract samples that involve control information interaction.

7. References

[1] Guo Zhengrong and Zhou Cheng 2004 *Working process and application of SSL protocol[J]. Network security technology and Application* pp 55-57
[2] Chen Hongxing and Zhou Yuanlan 2012 *Research on network information security countermeasures based on asymmetric encryption. Network security technology and Application* pp 20-22
[3] Shen Changxiang and Zhang Huanguo 2010 *Research and development of Trusted Computing [J]. Chinese Science： Information Science* pp 139-166
[4] Sun Yong and Chen Wei 2006 *Trusted computing in embedded systems[J]. Information security and communication secrecy* pp 50-52
[5] He Changduan and Chen Shuguo 2016 *Analysis of abnormal network communication in Smart Substation [J]. Electrical technology* pp 135-138
[6] Song Lei and Luo Qiliang 2004 *Encryption scheme for real-time data communication in power system [J]. Power system automation* pp 76-81
[7] Jia Jing 1999 *Security and secrecy of information system* p 150
[8] Li Xichun and Yao Weigang 2008 *Application and security of power data network. Jiangsu Electrical Engineering* pp 8-10
[9] Liu Shimin and Fan Rui 2015 *Research and application of intelligent substation online monitoring system. Electrical technology* pp 132-134
[10] Xu Weifeng and Zhang Hong 2007 *Construction of network information security for electric power enterprises.Shaanxi Electric Power* pp 75-77
[11] Zhang Liang and Xu Dianguo 2014 *An improved ant colony routing algorithm for low voltage power line communication. Transactions of China Electrotechnical Society* pp 318-324
[12] Gu Zhiru and Tan Zhouwen 2014 *Noise suppression of narrowband OFDM communication system in Smart Grid. Transactions of China Electrotechnical Society* pp 269-276