Research and Application of Substation Safety Communication Based on MMS Alternative Protocol

Huafeng Luo$^{1,a}$, Yifei Shen$^{1,b,*}$, Ai Xu$^{2,c}$, Chengyu Lu$^{1,d}$, Lixiang Ruan$^{1,e}$, Qiwei Du$^{1,f}$

$^1$State Grid Zhejiang Electric Power Co. Ltd. Research Institute, Hangzhou, Zhejiang, China
$^2$Beijing Sifang Engineering Technology Co. Ltd, Beijing, China
$^3$State Grid Zhejiang Electric Power Co. Ltd, Hangzhou, Zhejiang, China

$^a$email: luohuafeng2014@126.com, $^b$email: shen_yifei@zj.sgcc.com.cn, $^c$email: syf_sh188@163.com, $^d$email: 736932037@qq.com, $^e$email: 13857156066@163.com, $^f$email: zjsddqw@163.com

* Corresponding author’s e-mail: shen_yifei@zj.sgcc.com.cn

Abstract: At present, most substations are constructed based on IEC 61850 standard. The communication protocols in the station mainly include MMS, GOOSE and SMV, which are gradually exposed in engineering practice. Some deficiencies and potential safety hazards have emerged. For this reason, based on the MMS alternative protocol, the function and security of its implementation are introduced. In terms of functions, MMS alternative protocol adds multiple services and optimizes the deficiencies of the existing MMS protocol; for security, the application layer of the MMS alternative protocol implements two-way identity authentication based on the SM2 algorithm and despatching certificate, preventing unauthorized devices to prevent illegal access and attacks from the source of protocol; the transport layer of the MMS alternative protocol implements full link encryption and authentication based on the SM2 algorithm and despatching certificate to ensure the transmitted data message is antiforgery and non-repudiation and antitheft, protect the confidentiality and integrity of data messages. Therefore, the MMS alternative protocol has been greatly optimized on function, and the security authentication and transmission encryption mechanism of the protocol are focused on the security aspect. The final experimental results prove that the MMS alternative protocol has a certain reference significance in engineering applications.

1. Introduction
With the rapid development of information technology, network security of power information system in China has made some achievements, but some security risks have also been exposed$^{[1,2]}$. Vigorously developing independent and controllable, safe and reliable software and hardware technologies is an important solution to China's key software and hardware infrastructure. There are some key core technologies, such as developing independent and controllable processor, operating system, database, security encryption algorithm$^{[3,4]}$. In recent years, the State Grid Corporation of China has put forward a new generation of independent controllable safety protection measures for substation secondary system. At the same time, a series of technical specifications and standards are formulated, which mainly used to realize the independent control of software and hardware of secondary equipment in substation.
The status quo of key software and hardware technology and products dependence abroad can be get rid of as soon as possible.

At present, there are many researches on substation system security protection in China: In reference [5], a lightweight message authentication scheme for substation is proposed, which realizes the confidentiality, integrity and availability of communication between substation equipment by establishing authentication authority and control center. Reference [6] is based on the implementation of secure transmission technology of secure transport layer (TLS) protocol. By simplifying the steps of TLS protocol, the efficiency of establishing secure connection of TLS protocol is improved. IEC 62443 is the mainly standard about information security of industrial control system in foreign, while power system security mainly refers to IEC 62351 [7].

Most of the existing smart substations are built based on IEC 61850 standard. And IEC 61850 standard has great advantages in serving the construction and application of substations. Due to the wide application of intelligent devices information transmit mostly through TCP / IP or UDP in the substation, the communication system of the substation will face great security risks and hidden dangers [9-10]. IEC 62351 standard is an important reference standard for substation security protection at home and abroad. The core content of IEC 62351 standard is authentication and encryption, which covers the security reinforcement of protocol communication based on MMS, goose and SMV [11-13].

The MMS protocol defined in ISO / IEC 9506 standard is the application layer communication protocol for industrial automation system. And it’s the communication mapping specification between station control layer and bay layer in IEC 61850 standard [14]. However, there are some shortcomings and drawbacks in the process of engineering application. For example, there is no authentication mechanism in the association process of MMS protocol and MMS protocol message using plaintext transmission, etc. Based on MMS alternative protocol, this paper focuses on the security protection technology of MMS alternative protocol——A safe communication between devices in substation based on SM2 algorithm and dispatching certificate technology. In particular, the MMS replacement protocol described in this paper is only used to replace the original MMS communication protocol, excluding goose and SMV protocols. The alternative protocol is derived from the technical specification for the secondary system of the new generation of independent and controllable substations.

2. Brief introduction of MMS alternative protocol

MMS alternative protocol is a part of the software and hardware independent control technology of substation secondary equipment recently proposed by State Grid Corporation of China. It is committed to solve the problems and deficiencies of MMS protocol in the practical application process. Aiming to improve the security of the protocol, and solve the long-standing network security problems of communication system in substation.

MMS substitution protocol proposes a method of mapping IEC 61850 ACSI directly to TCP/IP protocol subset, which redefined the MMS mapping specification adopted in IEC 61850. It eliminates ACSE layer, session layer and tp0 layer of MMS stack. The hierarchy of MMS alternative protocol stack is shown in Figure 1.

| IEC 61850 ACSI Protocol Specification of DL/T 860 |
|-----------------------------------------------|
| Presentation Layer                             |
| ASN.1 PER (ISO 8825-2)                         |
| TCP/IP                                        |

Figure 1. Hierarchical structure of MMS alternative protocol stack

MMS alternative protocol maps more than 50 ACSI services defined in IEC 61850-7-2 (ED 2.0) to services with the same name. Adds two new services about AssociateNegotiate and Test. At the same time, the MMS alternative protocol expands the communication service of IEC 61850-7-2. Such as adding association negotiation service, functional constraints of data service, file service breakpoint
continuation, etc.

One to one mapping between MMS alternative protocol service and ACSI service enhances the readability of message. Test service is a new mechanism used to detect whether the communication link of application layer is normal. However, MMS protocol has no special test message, and the test service needs to occupy a certain network bandwidth, which increases the packet processing load. The newly added Association negotiation service is used to solve the security problem of MMS alternative protocol, that is, to realize the two-way identity authentication mechanism based on SM2 algorithm and dispatching Certificate in the application layer. The data packets based on TCP protocol provide encryption transmission mechanism based on encryption security suite which called TLS protocol with ECDHE_SM4_SHM3 [15] and ECC_SM4_SM3 in the transport layer.

Based on the above analysis, this paper focuses on the security communication technology between devices in Substation Based on MMS alternative protocol. The security protection of substation communication system realizes based on SM2 algorithm and dispatching certificate.

3. Autonomous controllable cipher algorithm and dispatching certificate application

At present, SM2 algorithm and dispatching certificate based on x509 specification have been applied to different business systems of the State Grid. This paper mainly uses SM2, SM3, SM4 algorithm [16-18] and dispatching certificate, based on MMS alternative protocol to complete the safe communication of substation system. The cryptographic application architecture is shown in Figure 2. As can be seen from Figure 2, the company password application system is composed of four levels. The bottom layer of cryptographic algorithm layer mainly provides algorithm support. The device support layer mainly integrates algorithms into hardware devices in the form of software and hardware. The supporting system layer mainly provides cryptographic services based on key management and digital certificate. The application system layer includes the specific business system in the electric power system.

Figure 2. Application architecture of power grid password

3.1 Application of SM2 algorithm signature

In the signature application of SM2 algorithm, data signature values generated from the signer. And verifies the reliability of the signature value by the verifier. The signer has a private key and a public key. The private key is used to generate the signature and the public key is used to verify the signature. The verifier obtains signer's public key so that the signature value can be verified. In information system, SM2, SM3 and SM4 algorithms are usually used together. For example: the identity authentication based on communication protocol needs combined usage with SM2 and SM3 algorithms. SM3 algorithm is used to calculate the hash value of the protocol packet, and calculate the signature value of the hash value by the algorithm of SM2. SM4 is used to protect the confidentiality of key business
data. And the dynamic key transmission of SM4 needs the encryption protection of SM2. The digital signature and verification process of SM2 algorithm is shown in Figure 3.

![Digital signature and verification process of SM2 algorithm](image)

Figure 3. Digital signature and verification process of SM2 algorithm

3.2 Dispatching certificate system

Dispatching certificate system is an important security infrastructure of power system. It provides security technical support for key security equipment, servers and operators of power system, including strong identity authentication of key links of power system and secure data transmission. The architecture of dispatching certificate system is shown in Figure 4. Certificate Authority (CA) is the top organization that issues certificates.

![Architecture of dispatching certificate system](image)

Figure 4. Architecture of dispatching certificate system

4. Secure communication technology in Substation Based on MMS alternative protocol

In China, the substation communication system based on IEC 61850 standard does not adopt credible security mechanism, but takes some security reinforcement measures on the basis of operating system, database and related middleware. Just like, designing complex login password, not opening useless ports, etc. But all these measures are only for the security reinforce about host and device body.

The security of communication protocol in substation is an important part of network security of power monitoring system. The following will focus on the security mechanism of MMS alternative protocol and the security protection mechanism based on SM2 algorithm and dispatching certificate technology.
4.1 Identity authentication mechanism in application layer of MMS alternative protocol

MMS protocol completes the connection process through three-time handshake of TCP. There is no corresponding security mechanism in the association process of application layer. And MMS alternative protocol can solve this security problem (It should be noted that the security risk here refers to that there is no identity authentication mechanism between devices which based on traditional MMS protocol communication. That is, any device can communicate with another device when access in the MMS communication network. It is easy for attackers to misuse their identities). There are authentication parameters in the syntax definition of associated request and response of MMS alternative protocol, which include signature certificate, signature time and signature value. Based on these parameters and SM2 algorithm, the security association process of MMS alternative protocol can be realized.

The syntax definition about association request and response of MMS alternative protocol can be seen in the Figure 10. AuthenticationParameter in syntax represents the security authentication associated with the application layer. Associationid represents the identity of the application layer Association. When secure communication is needed, authentication parameter should carry relevant information of dispatching certificate. The signatureCertificate is octet string (8-bit string). In the process of association establishment, the association requester assigns its signature certificate to the signatureCertificate. After confirming the legal identity of the association requester, the association responder assigns its signature certificate content to the signatureCertificate and sends it back to the association requester. Signedtime is the UTC time generated by the authenticationParameter, which represented by utctime type. And the time precision should be less than 1s. Signedvalue is calculated by the initiator (both client and server can be the initiator). And associated receiver verifies the IEDname and Accesspoint. In the calculation, only the signedtime data will be signed.

The security authentication process of communication parties based on MMS alternative protocol is shown in Figure 5. Through the security process design of client and server in Figure 5, the two-way identity authentication from client to server is realized. Any access device without security authentication can not communicate on the network, which eliminates the illegal access and attack of unauthorized devices.

![Figure 5. Two-way security authentication process](image-url)
4.2 Security mechanism in transport layer of MMS alternative protocol

The security of transport layer data in MMS alternative protocol needs confidentiality and integrity protection based on TLS protocol. OpenSSL is one of the most widely used security components in the world. It is used in companies all over the world, and it is open source and free of charge. OpenSSL on the official website implements the TLS protocol, which belongs to the international algorithm, and does not meet the demand of independent and controllable power secondary system. Therefore, based on the open source OpenSSL security component, this paper adds independent controllable cryptographic algorithms SM2, SM3, SM4 and the supports for dispatching certificate. According to GM/T 0015-2012《Digital certificate format specification based on SM2 cryptographic algorithm》and GM/T 0024-2014 《SSL VPN technical specification》, the TLS protocol between SM2 algorithm and dispatching certificate is implemented. The architecture of GMSSL (national security component) supporting SM2 algorithm and TLS protocol is shown in Figure 6. It consists of application layer component, TLS security component, basic encryption component and encryption engine component.

Figure 6. Architecture of GMSSL security components

Extending autonomous controlled cryptographic algorithms and dispatching certificates in basic encryption components. And extending TLS protocol stack in TLS component. The handshake process of the extended TLS protocol is showed in Figure 7. TLS protocol consists of handshake and encryption. The main purpose of handshake is to obtain session key through negotiation. And the encryption process mainly uses the session key obtained by negotiation to encrypt communication. The TLS protocol itself allows the use of multiple cipher Suites for session key agreement. This paper uses ECDHE_SM4_SM3, ECC_SM4_SM3 encryption suite and dispatch certificate to realize the confidentiality and integrity of link data.
In summary, the complete secure communication flow of MMS alternative protocol is shown in Figure 8.

Figure 7. TLS protocol handshake process based on SM2 algorithm

Figure 8. Secure communication processes of MMS alternative protocol
The security of MMS alternative protocol is fully considered when MMS alternative protocol designed. In addition to adding two-way identity authentication in the application layer of the protocol, TLS protocol is also used in the transport layer for security protection. The security of protocol data transmission is guaranteed by security reinforcement at two different protocol layers. MMS alternative protocol eliminates the insecurity at the source of the protocol and protects the confidentiality and integrity of the data packets. And the feasibility of tampering, forgery and theft of protocol packets in any link during transmission is eliminated.

4.3 Engineering application of MMS alternative protocol
Based on the security protection technology of MMS alternative protocol, this section mainly introduces the engineering application of MMS alternative protocol. Figure 9 shows the security communication architecture of substation. It mainly including the security protection of station control layer and bay layer network.

![Security communication architecture of substation](image)

Figure 9. Security communication architecture of substation
There are dispatching certificates to identify themselves in both station control layer and interval layer devices. The equipment certificate is issued by the dispatching certificate system, which is used to identify the equipment. And it also used for the safe communication between the equipment. The association authentication of MMS alternative protocol is to realize mutual identity recognition based on device certificate. And the security about transport layer of MMS alternative protocol is also based on certificate and SM4 algorithm to realize the encryption of transport layer data.

In addition, due to the large number of equipment in the substation, special attention should be paid to the configuration of equipment certificates. The mismatch of equipment certificate, certificate expiration, key error, algorithm parameter error and so on, which will directly affect the communication of the system. And the amount of engineering implementation is large. It’s necessary for engineers to have a strict safety training.

5. Analysis of performance and security

5.1 Timeliness analysis of MMS alternative protocol for two-way identity authentication
The two-way identity authentication of MMS alternative protocol is a security mechanism implemented in the application layer of the protocol after TCP connection, its main purpose is to prevent the protocol from being forged, tampered and repudiated. According to the test purpose, the test platform is built, and the configuration information of software and hardware resources is shown in Table 1.
Based on the above test environment, we perform four associated operations respectively. In order to verify the situations about security authentication mechanism of MMS alternative protocol application layer, and compare the security association and non-security association in the association service. The results are shown in Table 2. It can be seen from table 2 that the increased time of security association mode than that of non security association mode is at millisecond level. The authentication process is mainly the signature and verification operation of SM2 algorithm, as the SM2 algorithm is highly efficient, and the execution of associated operations is not frequent. Therefore, the timeliness of MMS alternative protocol application layer security authentication mechanism meet the business requirements.

5.2 Analysis of TLS protocol encryption timeliness

TLS protocol includes handshake protocol and record protocol. The handshake protocol is mainly used for the identity authentication, algorithm and key agreement between the two sides, and finally generates the session key. The recording protocol is mainly used for grouping, encrypting and decrypting data packets by session key.

In the first phase of TLS protocol, two-way authentication and key agreement are needed. Therefore, it will take longer to initialize the connection than non secure communication (increasing about 410-430 ms, the actual delay is related to the CPU, memory and operating system of the device). In addition, the initialization connection is not frequently required. The time-consuming results of four TLS connections are shown in Table 3. The average time-consuming is 414.25ms.

6. Conclusion

Under the background that China vigorously promotes the independent control of key basic technologies and the State Grid Corporation promotes the independent control of software and hardware tech-
nologies of power secondary system. In this paper, the shortcomings and security risks of MMS protocol in practical engineering application are indicated, and it is improved and perfected in the new MMS alternative protocol.

Based on MMS alternative protocol, the security authentication mechanism of the protocol is implemented from the source. For perfecting security protection mechanism, independent and controllable cryptographic algorithm, dispatching certificate and TLS protocol are adopted. In the application layer of the protocol, the identity authentication function of both sides of the communication is implemented. It can preventing protocol data from being forged and tampered in the process of transmission, and ensuring the anti-repudiation and integrity of protocol data transmission.

This paper also tests the timeliness of the associated security authentication and transport layer security protection of MMS alternative protocol. From the experimental results, these following conclusions can be drawn: ① The associated security authentication in application layer takes milliseconds, which meet the business requirements; ② The timeliness of encryption based on TLS protocol in transmission layer has a certain impact on the efficiency of substation business data transmission, which is optional according to the actual situation of business security requirements. In addition, consider from operation maintenance and management of substation system, the security mechanism of substation system involves the management of many dispatching certificates and keys, Therefore, it is necessary for further study on its popularization and application.

7. Appendices

Figure 10. Syntax definition of association authentication

Acknowledgments
This paper is one of the phased results of the Science and Technology Project of State Grid Zhejiang Electric Power Co. Ltd. (5211DS19002W)《Research and application of MMS communication security system for intelligent substation monitoring system》. And I would like to express my gratitude to all those who helped me during the writing of this paper. Thanks for your support!

References
[1] Liu K, Huang M.H, Li Y.Q, et al. (2018) Fault information model and online monitoring method for relay protection system in smart substation. Electric Power Automation Equipment, 38(2):210-216.
[2] Peng Z.Q, Zhang Q.B, Su D.W, et al. (2019) Remote operation and maintenance technology of
substation supervisory control system based on GPS. Electric Power Automation Equipment, 39(4):210-216.

[3] Qi Z.Y, Chang P.P. (2020) Opportunities and challenges of domestic operating system. Computer knowledge and technology, 16(14):246-247.

[4] Zhang Y.J. (2019) Analysis of the environment of autonomy and controllability in our country. Electronics Quality, (7):58-61.

[5] Zhang J.H, Zhang Y, Shen Y, et al. (2018) An efficient and secure lightweight message authentication scheme for smart substation. Smart Power, 46(11):53-58.

[6] Fang F, Wang D.H, Xuan X.H, et al. (2019) Research on telecontrol communication of smart substation based on TLS connection. Electric Engineering, (8):75-77.

[7] Zhang L.H, Liu K.S. (2019) Summary and reflection on safety standards of typical industrial control systems at home and abroad. Technology innovation and application, (26):81-82, 85.

[8] Ren Y.M, Cao F.M, Tang X, et al. (2011) Advice on communication standards for smart grid. Automation of Electric Power Systems, 35(3):1-4, 61.

[9] Zhang X.M, LI J, Qiu R.F, et al. (2020) Research and application of national cryptographic series technology in smart substation. Southern Power System Technology, 14(1):39-45.

[10] Xu A, Liu G, Xu Y.M. (2018) Security protection technology of smart substation based on SM9 identity-based cryptographic. Automation Panorama, 35(Supplement 2):65-71.

[11] Cleveland F. (2006) IEC TCS57 security standards for the power system's information infrastructure beyondd simple encryption/Transmission & Distribution Conference & Exhibition. Dallas, TX, USA: IEEE, 1079-1087.

[12] International Electrotechnical Commission. Power systems management and associated information exchange-data and communications security-part 3:communication network and system security-profiles including TCP/IP:IEC 62351-3-2014[S]. [S.l.]: AENOR,2014.

[13] International Electrotechnical Commission. Power systems management and associated information exchange-data and communications security-Part4: security for profiles including MMX and similar payloads: IEC CDV 62351-4-2017[S]. [S.l.]: AENOR, 2017.

[14] Gong J.Q, Huang Y.Z, Xia M.C. (2004) Application of MMS in IEDs of power system [J]. Electric Power Automation Equipment, 24(6):72-75.

[15] National Password Agency ( 2014 ). SSL VPN technical specification. https://www.doc88.com/p-9029134947623.html

[16] General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization administration. (2017) Information Security Technology SM2 Elliptic Curve Public Key Cryptography Algorithm. Standards Press of China, Beijing.

[17] General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization administration. (2017) Information security technology SM3 cipher hash algorithm. Standards Press of China, Beijing.

[18] General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization administration. (2017) Information security technology SM4 block cipher algorithm. Standards Press of China, Beijing.

[19] Zheng X, Yin J.J, Du Q.W, Yin H, Ruan L.X. (2021) Operation and Maintenance Control System for Substation Automatic Equipment and Its Application. Zhejiang Electric Power, 2021, 40(03):42-50.