J. Mod. Power Syst. Clean Energy (2019) 7(4):948–961
https://doi.org/10.1007/s40565-019-0498-5

A security scheme for intelligent substation communications considering real-time performance

Jie ZHANG[1], Jun'e LI[1], Xiong CHEN[2,3,4], Ming NI[2,3,4], Ting WANG[1], Jianbo LUO[2,3,4]

Abstract Tampering, forgery and theft of the measurement and control messages in a smart grid could cause one breakdown in the power system. However, no security measures are employed for communications in intelligent substations. Communication services in an intelligent substation have high demands for real-time performance, which must be considered when deploying security measures. This paper studies the security requirements of communication services in intelligent substations, analyzes the security capabilities and shortages of IEC 62351, and proposes a novel security scheme for intelligent substation communications. This security scheme covers internal and telecontrol communications, in which the real-time performance of each security measure is considered. In this scheme, certificateless public key cryptography (CLPKC) is used to avoid the latency of certificate exchange in certificate-based cryptosystem and the problem of key escrow in identity-based cryptosystem; the security measures of generic object-oriented substation event, sampled measure value and manufacturing message specification in IEC 62351 are improved to meet the real-time requirements of the messages as well as to provide new security features to resist repudiation and replay attacks; and the security at transport layer is modified to fit CLPKC, which implements mutual authentication by exchanging signatures. Furthermore, a deployment of CLPKC in an intelligent substation is presented. We also evaluate the security properties of the scheme and analyze the end-to-end delays of secured services by combining theoretical calculation and simulation in this paper. The results indicate that the proposed scheme meets the requirements of security and real-time performance of communications in intelligent substations.

Keywords Intelligent substation, Security measures, Certificateless public key cryptography (CLPKC), Real-time communication, IEC 62351

CrossCheck date: 27 November 2018

Received: 3 May 2018 / Accepted: 27 November 2018 / Published online: 1 February 2019
© The Author(s) 2019

✉ Jun'e LI
jeli@whu.edu.cn

Jie ZHANG
zhangjie0614@163.com

Xiong CHEN
chenxiong@sgepri.sgcc.com.cn

Ming NI
ni-ming@sgepri.sgcc.com.cn

Ting WANG
phoebe_0727@163.com

Jianbo LUO
luojianbo@sgepri.sgcc.com.cn

[1] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

[2] NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China

[3] NARI Technology Co. Ltd., Nanjing 211106, China

[4] State Key Laboratory of Smart Grid Protection and Control, Nanjing 211106, China

1 Introduction

With the development of intelligent substations, the communication of substations gradually developed from point-to-point connections to networked connections. Intelligent substations are facing increasing cyber security threats. However, both internal and telecontrol communications of built intelligent substations have not employed any security measures so far [1]. Messages such as sampled value messages and protection control messages can easily be tampered, forged or stolen due to the lack of integrity verification, authentication or encryption. The security of communication services has a profound impact on the reliable operation of primary devices. The attack of messages may cause faults in the power system and cause inestimable losses. A typical case is the large-scale blackout in the Ukrainian grid caused by a cyber-attack at the end of 2015 [2]. Therefore, it is urgent to add security measures to communication networks in a substation.

Security measures cause extra computing cost and communication delay despite improving the communication security of intelligent substations. The measurement and control devices in intelligent substations are usually embedded systems, which have limited computing resources. Intelligent substations have high real-time requirements for communications, and the real-time performance of communications directly affect the reliable operation of the primary device. Therefore, when designing a security scheme for a substation communication network, we need to consider not only the security of the scheme but also its real-time performance.

To provide security assurance for communications in intelligent substations, the International Electrotechnical Commission (IEC) developed some security measures released in IEC 62351 [3]. The cyber-security of intelligent substations has also caused wide public concern in international academe. Reference [4] presented three weaknesses of IEC 62351 but without modification. Reference [5] presented a security mechanism based on galois/counter mode (GCM) to ensure communication security of intelligent substations, but the distribution and management of keys are very complicated. Reference [6] proposed a password authentication method based on chaotic theory, which has poor resistance for addressing plaintext attacks. In order to ensure the secure transmission of communication messages, reference [7, 8] proposed SM2-based security mechanisms, reference [9] designed a security mechanism that was mixed with encryption by DES and RSA, but both of them require high computing performance to satisfy the real-time requirements of substation communications, so they are not suitable for substation systems.

Some scholars studied encryption key management mechanisms for the smart grid, which can be classified in the following categories: key management schemes based on the symmetric-key [10], public key infrastructure (PKI) [11], identity-based cryptosystem (IBC) [12], and preinstalled keys [13]. However, each of these four key management mechanisms has its own weakness. The symmetric key is vulnerable to man-in-the-middle attacks; the mechanism based on PKI creates heavy loads in the communication network as well as delays in certificate exchange; the mechanisms based on IBC or preinstalled keys have the problem of key escrow. Beyond that, to avoid the delay of certificate exchange and reduce the load of the communication network, some scholars are trying to employ the method of a preinstalled certificate for a new device in view of the characteristic that the communication relationship is certain in smart substations, but it comes with the problem of certificate update.

In brief, though scholars have carried out extensive researches on the communication security of intelligent substations, there are various shortcomings in considering its characteristics, especially real-time requirements. In addition, no research so far has solved the problems of the latency of certificates exchanging, certificate management and key escrow in key management.

Therefore, aiming at the cyber threats of intelligent substations, this paper analyzes the security capabilities and shortages of IEC 62351 and presents an overall security scheme for intelligent substation communications taking into account real-time performance. In order to enhance the capabilities of substation communication in terms of confidentiality, integrity, authenticity, immunity against replay attack and non-repudiation, security measures for internal and telecontrol communications are proposed. Moreover, a key management method is designed based on certificateless public key cryptography (CLPKC) to avoid the delay of certificate exchange and the problem of key escrow. Finally, the evaluation of security properties and the analysis of end-to-end delays prove that the security measures in this paper can meet the requirements of security and real-time performance of substation communications.

2 Security requirements of intelligent substation and security capability of IEC 62351

2.1 Threats and security requirements of smart substations

Attacks on intelligent substations can be divided into two phases in terms of time: ① finding the appropriate attack path to access the communication network of

substations; ② attacking the communication network or important communication messages to cause abnormalities in the physical device, ultimately reaching the purpose of attacking the smart grid [14]. For the first phase, we can deploy physical isolation, a firewall and other measures in substations to block the attack path. Therefore, we study the threats and security requirements of communication services in the scenario that attackers have successfully accessed the substation's communication network.

At present, intelligent substations commonly adopt the structure of "three layers, two networks". The architecture shown in Fig. 1 is a typical framework of a substation's communication network. The data flows and their message types of communication networks are presented in Fig. 1.

The data exchanged between the substation level and the other substation or remote control center are primarily control instructions and original data files. The data exchanged between the substation level and bay level are control instructions, device status information and constant values. Manufacturing message specification (MMS) protocol is used in the aforementioned transmission services. These data may be tampered or forged to disturb normal operations of substations, and the status data may be stolen by attackers for future attacks. Therefore, it is necessary to ensure their confidentiality, integrity and authenticity.

The data communications, whether within the bay level or between the bay level and process level, are carried out through the process level network and primarily adopt the generic object oriented substation event (GOOSE) protocol or sampled measure value (SMV) protocol. The sampled value messages, from the merging unit (MU) to the protection and control (P&C) device, adopt the SMV protocol. Control instructions and switch status messages adopt the GOOSE protocol. These messages require high real-time performance. An attacker could control the continuity of a primary device or cause a malfunction of a primary device by tampering, forging or replaying messages, thereby causing the breakdown of the primary device or the instability of the smart grid. Stealing these messages makes little sense. Therefore, the security requirements of the above communication services include integrity, authenticity and availability, and no confidentiality.

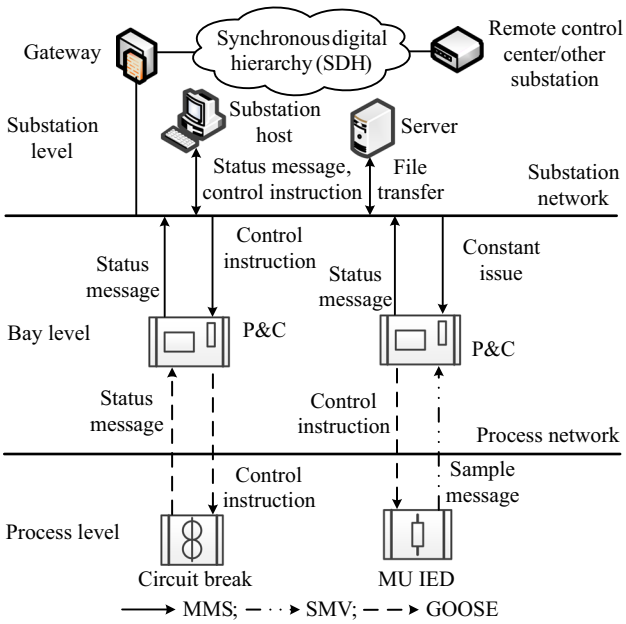

Fig. 1 Main data flows in an intelligent substation

In addition, current intelligent substations lack network monitoring and log audit so that the source cannot be traced. Therefore, they are vulnerable for repudiation attacks. Furthermore, all services in substations could suffer from denial of service (DoS) attacks that affect the availability of the substations' resources.

In brief, the main security threats of substations are unauthorized access, forgery, theft, DoS, and repudiation.

2.2 Security capabilities and shortcomings of IEC 62351

According to Section 2.1 and IEC 62351, security threats, requirements and capabilities of IEC 62351 for messages in substation communication networks can be summarized as shown in Table 1, which shows that the security capabilities of IEC 62351 cannot meet the security requirements of the substations.

There are also additional shortages in IEC 62351 as follows:

1) Key or certificate management has not yet been specified in IEC 62351 standards.
2) Some of the security measures specified in IEC 62351 have weaknesses that make them unsuitable for communication services in intelligent substations. As an illustration, the performance of the specified signature algorithm for the GOOSE and SMV messages cannot satisfy real-time requirements of substation communications because of the high complexity of the RSA.

3 Proposed security scheme for communications of intelligent substations

The security scheme includes security measures for communication messages and its key management method. The communications messages involve the internal and telecontrol communications of the substation system. The security measures are improvements to those in IEC 62351, and the key management method is based on CLPKC in

STATE GRID
STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

Table 1 Security threats, requirements and capabilities of IEC 62351 for messages in substations

Type of message	Security threats	Security requirements	Security capabilities of IEC 62351
GOOSE/SMV	Tampering, forgery, repudiation, DoS attack	Integrity, authenticity, non-repudiation, availability	Message authentication mechanism
MMS	Tampering, forgery, stealing, repudiation, DoS attack	Integrity, authenticity, confidentiality, non-repudiation, availability	Peer entity authentication, transport-profile security

this scheme. The main contents are as shown below: the security measures of GOOSE/SMV and MMS in IEC 62351 are improved in Section 3.1; the transport layer security (TLS) protocol is modified to fit CLPKC, and its handshake process of modified TLS is shown in Section 3.2; a deployment of CLPKC is presented in Section 3.3. The modified TLS is for both telecontrol communications and the low-speed messages of internal communications.

3.1 Security measures for internal communications of intelligent substations

The deployment of security measures for communications within a substation is shown in Fig. 2. Security measures proposed for GOOSE/SMV can be used to protect the communications within the bay level and the communications between the bay level and process layer (shown as the blue arrows in Fig. 2). Security measures proposed for MMS can be used to protect the communications within the substation level and the communications between the substation level and bay level (shown as the red arrows in Fig. 2).

3.1.1 Security measures for GOOSE/SMV

As discussed in Section 2.1, the security requirements of GOOSE/SMV are authenticity, integrity, availability and non-repudiation. Taking into account the same security requirements of the SMV and GOOSE protocols, this paper designs the same measures to protect GOOSE/SMV messages.

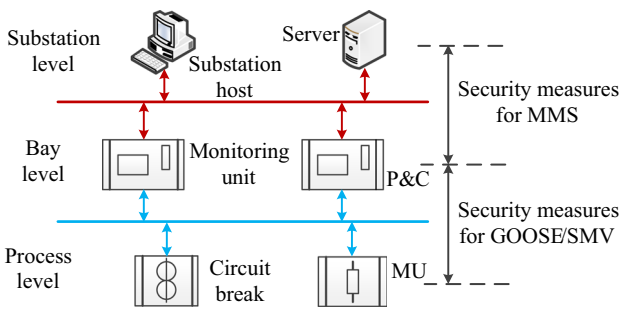

Fig. 2 Deployment of security measures within substation

According to IEC 62351-6, the reserved fields and extension fields in GOOSE/SMV are used to extend the function of GOOSE/SMV messages as follows:

1) The first byte of the Reserved1 field shall be used to specify the number of octets conveyed by the extension octets; the Reserved2 field shall contain a 16-bit cyclic redundancy check (CRC), the CRC shall be calculated over octets 1–8 of the VLAN information of the extended protocol data unit (PDU).
2) The extension shall be encoded; the authentication value field shall be used to store the signature value.
3) In order to prevent a replay attack, skew filtering and timestamp checking are proposed to distinguish current messages and outdated messages.

The security measures in IEC 62351 for GOOSE/SMV cannot resist repudiation. Therefore, this paper proposes that the unique identification on behalf of the identity of a device in a substation is added into the Reserved SEQUENCE field. Hence, the device cannot deny its participation in the communication. Moreover, considering the real-time requirement of GOOSE/SMV messages, a hash-based message authentication code (HMAC) algorithm is employed to calculate the signature value instead of the asymmetric RSA algorithm specified in IEC 62351, and the SHA256 algorithm is employed for the hash calculation. The specific authentication process of GOOSE/SMV is shown in Fig. 3.

3.1.2 Security measures for MMS

MMS is an application protocol based on TCP/IP. The security requirement of MMS includes confidentiality, integrity, authenticity, availability and non-repudiation as discussed in Section 2.1.

According to IEC 62351-4, the authenticity of MMS is provided by peer entity authentication that occurs at association set up time. The authentication is implemented through association control service element (ACSE) security as follows: enabling sender-ACES-requirements field and responder-ACSE-requirement field of the authentication functional unit (FU) of ACSE, defining the data

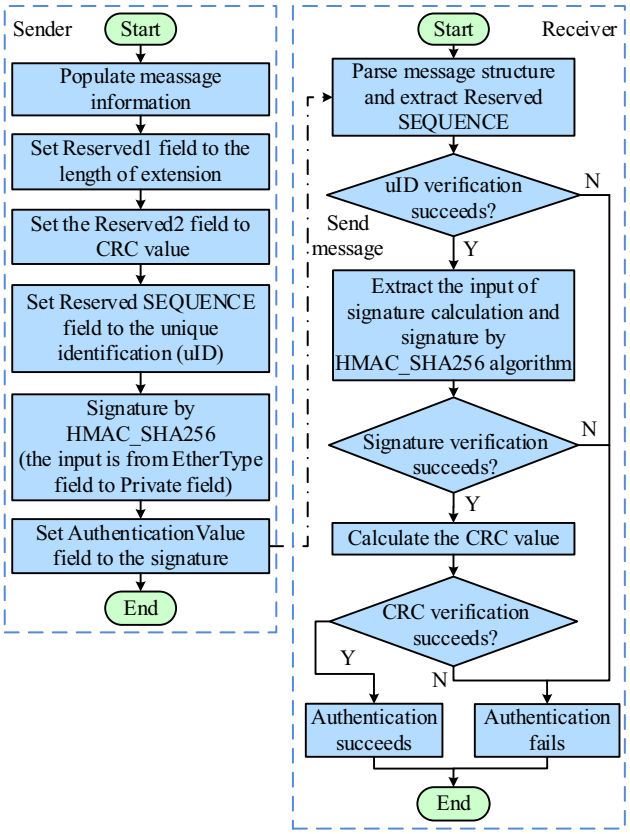

Fig. 3 Security authentication process of GOOSE/SMV

structure MMS_Authentication-value where the signature value is stored.

In order to improve the security measures in IEC 62351 for MMS in terms of integrity, non-repudiation and confidentiality, this paper proposes the following security measures.

To protect the integrity of MMS, this paper adopts the method of hashing the date of MMS messages by using a hash algorithm to prevent the unauthorized modification. Considering the requirements of intelligent substations for security and real-time performance, we select SM3 as the hash algorithm. To resist the repudiation attack, this paper proposes adding a unique identification of the device into the MMS message. The specific authentication process of MMS is shown in Fig. 4.

IEC 62351 suggests that the confidentiality of MMS is provided by TLS protocol but does not specify details about it, and TLS has deficiencies in real time. In addition, there are different communication services of MMS messages in intelligent substations, such as the device status message and file transfer message. The device status message is a medium-speed message whereas the file transfer message is a low-speed message. They have different requirements of real-time performance for communication services.

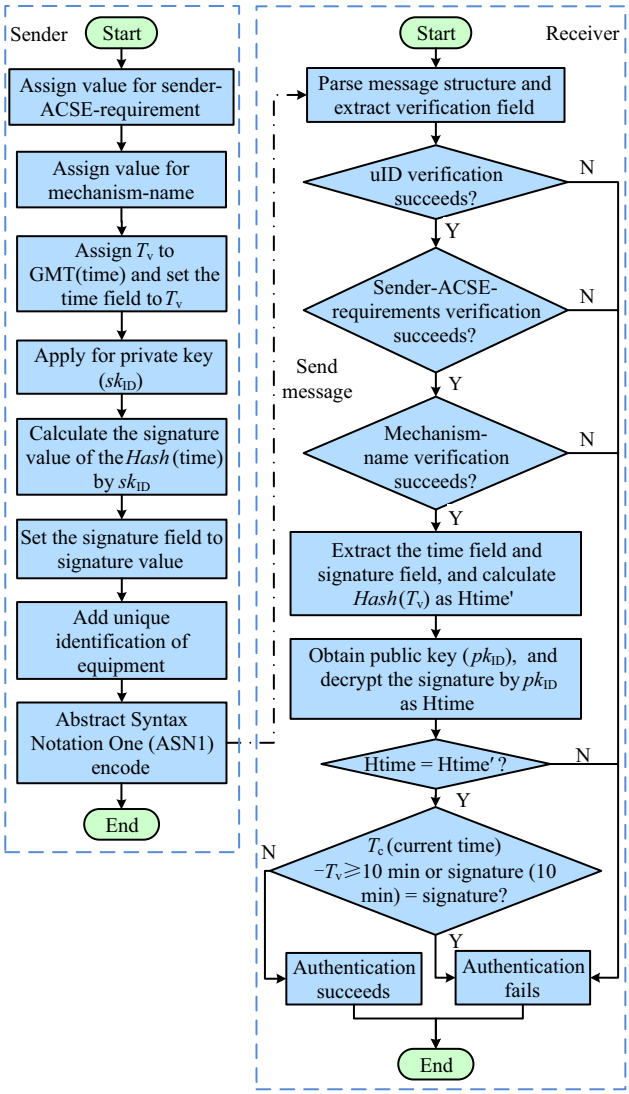

Fig. 4 Specific authentication process of MMS

Therefore, in this paper, different security measures are designed for different services of MMS messages to ensure their confidentiality after considering their real-time requirements: low-speed messages adopt the modified TLS proposed in this paper; medium-speed messages adopt the method of signature-then-encryption on the sending side and decryption-then-authentication on the receiving side. Compared with the RSA algorithm, SM2 has the advantages of higher security, faster operation, and less resource consumption, so we select SM2 as the algorithm of authentication and encryption.

3.2 Security measures for telecontrol communications

The deployment of security measures for telecontrol communications is shown in Fig. 5. The challenge-

STATE GRID
STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

response mechanism is adopted to protect the communications between the two substations. The modified TLS protocol, which achieves mutual authentication by exchanging signatures instead of digital certifications, is used to protect the communications between the substation and remote control center.

3.2.1 Challenge-response mechanism

Challenge-response provides the authentication for the application layer. According to IEC 62351-5, the role of a substation can be a challenger or a responder for one inter-station communication connection. When inter-station operations are associated with specific application service data units (ASDUs) that the challenger considers to be protected, the challenge-response authentication mechanism based on HMAC will be used. The authentication process is shown in Fig. 6.

3.2.2 Modifications to TLS

Both of the communications between two substations and the communications between a substation and remote control center primarily use TCP/IP. TLS can be used to protect telecontrol communications. In order to fit CLPKC, TLS shall be modified as follows: mutual authentication is completed by exchanging the signature instead of using digital certification, so as to avoid the impact of certificate exchange on real-time performance of the communication.

Depicted in Fig. 7, the handshake of our modified TLS consists of the following three steps:

Step 1: Start handshake.

1) Client sends ClientHello message to server, which contains version, random value a, session_id, and cipher_suites, etc.
2) Server responds client with ServerHello message, which specifies negotiated parameters and contains random value b.

Step 2: Implement mutual authentication between server and client.

1) Server selects a random plaintext M, and the signature $S = Sig(S_{sk}, Hash(M))$ is calculated with the private key (S_{sk}) of server. Then, server sends M and S to client by ServerAuthenicate message.
2) Server sends AuthenticateRequest message to client to request authenticating the identity of client.
3) Client calculates $H = Ver(S, S_{pk})$ with the server's public key (S_{pk}) and judges whether the identity of server is legal by comparing H with $Hash(M)$. Then, client calculates $S' = Sig(C_{sk}, Hash(M))$ with the client's private key (C_{sk}) and sends S' to server.
4) Server calculates $H' = Ver(S', C_{pk})$ with the client's public key (C_{pk}) to verifies the identity of client.

Step 3: Negotiate session key and finish handshake.

1) Client generates a random number N_{pm} and generates session key SK with a, b, and N_{pm}. Then,

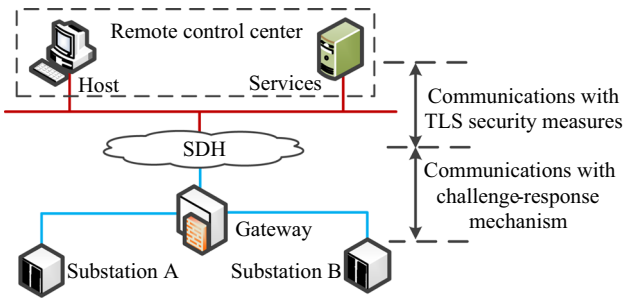

Fig. 5 Deployment of security measures for telecontrol communications

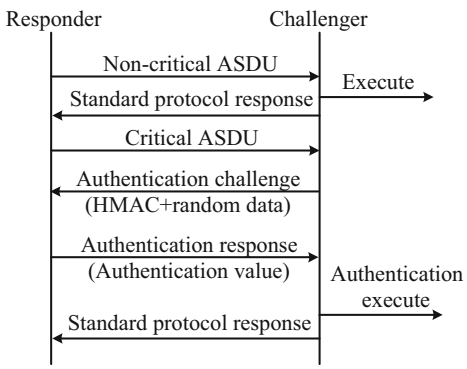

Fig. 6 Process of challenge-response authentication

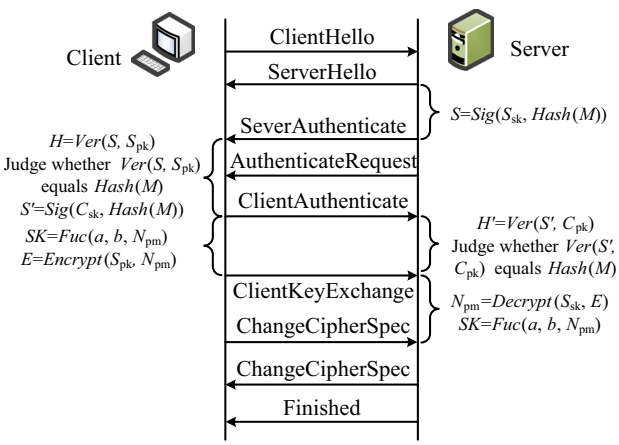

Fig. 7 Handshake process of modified TLS protocol

$E = Encrypt(S_{pk}, N_{pm})$ is calculated and sent to the server, where $Encrypt(\cdot)$ is the encryption function.

2) Server decrypts E by using the decryption fuction $Decrypt(\cdot)$ to obtain $N_{pm} = Decrypt(S_{sk}, E)$, and then, server calculates the session key SK with a, b and N_{pm} using the function $Fuc(\cdot)$.
3) Client and server verify the handshake channel, if success, both sides exchange communication data by SK. Then, they indicate that they have switched to encryption mode by ChangeCipherSpec message and finish the handshake through Finished message.

To ensure the security of the communication process, this paper suggests SM2 as the signature algorithm for authentication and the encryption algorithm for encrypting the session key. The advanced encryption standard (AES) algorithm is used to encrypt the session data, and the SHA256 algorithm is used to calculate the message digest.

3.3 Scheme of key management

PKI has been widely used in large-scale public networks, but the certificate management for enormous intelligent electronic devices (IEDs) in substations and the exchange of certificates would result in huge communications costs. The research on IBC is still undergoing and the revocation and escrow of keys are unsolved in IBC. Therefore, considering the characteristics of communications in smart substations and the requirements of messages for real-time performance, this paper proposes employing CLPKC in substations and presents a method of key update based on time validity.

3.3.1 Deployment of CLPKC in substation

In CLPKC, the generation of the user's public key is not completely based on its identity information, and the key generation center (KGC) does not know the user's whole private key. CLPKC does not require manage certificates and therefore effectively solves the key escrow problem. At present, there are various models of CLPKC [15–19]. Considering the characteristics of substation communications, after comparing the existing CLPKC models, this paper chooses the model in [18] for the scheme and a deployment in a substation system based on the following proposal.

In this scheme, KGC uses a centralized-distributed architecture, which should be first established in the power system. The detailed process of a device obtaining a pair of public keys and private keys consists of the following four steps.

Step 1: The upper KGC generates public parameters (s_{pk}) and master key (s_{mk}) randomly for every substation.

Step 2: When a device applies for key, the underlying KGC in the substation generate part private key (d_{ID}) and partial public key (p_{ID}) with s_{pk}, s_{mk} and device's identifier ID, and sends d_{ID} and p_{ID} to the device through the secure channel.

Step 3: The device generate a secret value (x_{ID}) with s_{pk} and ID, and generate a public key (pk_{ID}) with s_{pk}, p_{ID} and x_{ID}. Then the device publishes pk_{ID} out in the substation.

Step 4: Taking s_{pk}, d_{ID} and x_{ID} as input, the device generate the private key (sk_{ID}).

The security process based on this deployment of CLPKC in substation is shown in Fig. 8.

3.3.2 Key updating method

To ensure the availability of the public key in a certain period, the traditional public key cryptography binds the user to the public key by certification authority (CA) certification, and the cryptographic key of the user is bound to their identification information in the CLPKC. In order to complete the key management scheme, this paper considers the characteristics of substation communications and chooses the method in [20] for the key update. The preset time validity shall be attached to the user's identity to achieve the update and revocation of the key. For example, if the public key of device A in a substation is (A_Identity, spk) ‖ current-day, it means that A needs to update its key every day, otherwise the key will automatically expire. One could potentially make this approach more granular by changing the preset time validity. The shorter the time validity is, the higher the frequent update will be, and the more secure the cryptographic key will be. But frequent updates of cryptographic keys will increase communication latency. Therefore, the update frequency requires consideration of the real-time requirements of various communication messages in practice. On the premise of satisfying the real-time performance of the communication, the frequency of the key update increases. This will be considered in a future work.

3.4 Scheme security analysis

Security of the proposed scheme is analyzed from the following two aspects.

3.4.1 Security of measures

1) Integrity and authenticity: in this scheme, the AuthenticationValue filed in the GOOSE/SMV message is enabled with signature authentication based on

STATE GRID
STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

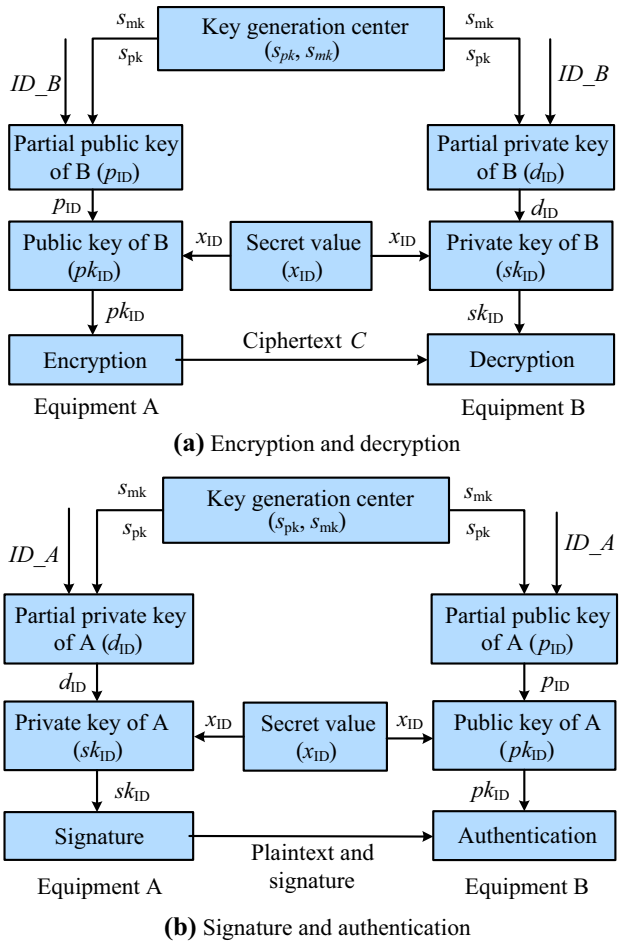

Fig. 8 Certificateless security processes

the HMAC algorithm to ensure the integrity and authenticity of GOOSE/SMV messages, which prevents the data from being tampered or forged during the transmission. Furthermore, we define the data structure of the Authentication value of MMS and adopt peer entity authentication based on the SM2 algorithm to verify the integrity and authenticity of MMS messages. The method of hashing the date of MMS messages by the SM3 algorithm can prevent an unauthorized modification. By this way, attackers cannot arbitrarily tamper or forge messages.

2) Confidentiality: in the scheme, as for different types of MMS messages, different measures are designed to ensure the confidentiality of message transmissions. Modified TLS protocol is adopted to ensure the confidentiality of low-speed messages, whereas medium-speed messages adopt the encryption algorithm to ensure their confidentiality. These measures can effectively prevent data from being stolen.
3) Non-repudiation: the unique identification of the sender is carried in the Reserved SEQUENCE field of messages to ensure that the device cannot deny its participation in the communication, which effectively resists a repudiation attack.
4) Immunity against replay: skew filtering and timestamp checking are used to distinguish the current packages and outdated packages, which effectively prevent a replay attack.

3.4.2 *Security of key management*

Considering the disadvantages of PKI and IBC, we propose employing CLPKC in substations. As an important part of the security scheme, the security of the key management is crucial. In the idea of security for CLPKC, there are two types of adversaries, type I and type II. The type I adversary A_{I} does not have access to the master key but it may replace the public key of arbitrary identities with values of its own choice, whereas the type II adversary A_{II} does have access to the master key but may not replace the public keys of entities. In the deployment of CLPKC in substations in this paper, the private key is not only related to a secret value but also to a partial private key obtained from the KGC, and the secret value is not transmitted through the channel. It is secure against type I and type II adversaries in a strong sense, provided that the computational Diffie-Hellman problem is intractable and the underlying hash functions are the random oracles [17].

4 Analysis for real-time performance of scheme

4.1 Composition of communication delay

The end-to-end delay of a message across the secured network with the proposed security measures primarily includes the following four parts, as shown in Fig. 9.

1) Generating delay (T_{G}) and parsing delay (T_{P}): the time that the sender generates and encapsulates the message from application layer to physical layer, and the time that the receiver parses and extracts the message from physical layer to application layer.
2) Delay of security operations (T_{E}): the computing time of security measures and the delay of transmissions between the security chip and master CPU.
3) Sending delay (T_{S}) and receiving delay (T_{R}): the time that the sender sends all of the packet's bits into the wire and the time that the receiver receives all of the packet's bits from the wire, which is defined the same as usual. This is the delay caused by the data rate of the link.
4) Link transmission delay (T_{L}): the amount of the propagation delay on the links and the processing

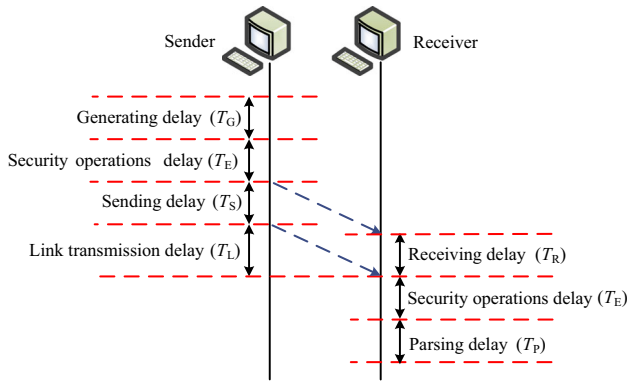

Fig. 9 Composition of message communication delay in secured substation network

and queuing delay in forwarding nodes from source to destination.

According to the above analysis, the end-to-end delay T of messages in intelligent substations is as follows:

$$T = T_{\mathrm{E}} + T_{\mathrm{other}} \tag{1}$$

where T_{other} is the delay in addition to the delay of security operations:

$$T_{\mathrm{other}} = T_{\mathrm{G}} + T_{\mathrm{S}} + T_{\mathrm{L}} + T_{\mathrm{P}} \tag{2}$$

Current simulation software cannot support the simulation of the proposed security operations. It is difficult to embed the security operation implementations to the existing simulation software, and the workload is too large to implement an entire simulation system. Therefore, the method of combining the theoretical calculation with the simulation is used to analyze end-to-end delays in this paper. The delay of security operations is calculated through theoretical analysis and the other delays are obtained by simulation in the software.

4.2 Calculation of security operation delays

Due to the high real-time requirement of intelligent substation communication, security chips are used to support security measures in our security scheme. After detailed analysis and comparison of various security chips, we selected A980 chip as a practical choice for analysis. The calculation rates of partial algorithms of A980 are shown in Table 2, in which the unit tps signifies times per second.

4.2.1 *Analysis for security operation delay of GOOSE/SMV*

According to Fig. 3, the authenticating process of GOOSE/SMV includes a CRC, digest calculation and signature calculation. The calculating length of CRC is 8 bytes, which is ignored here because of the simplicity of CRC. The length of a GOOSE/SMV message varies when it transmits different types of information. In this paper, the delays of the sampled value message, trip message and switch status message are analyzed. These messages have the highest real-time requirements. Large lengths of these messages are configured in the analysis: sampled value message is 159 bytes, trip message is 113 bytes, and switch status message is 256 bytes. The input length of signature calculation cannot exceed 240 bytes. Therefore, the operation delay of the digest calculation of the GOOSE/SMV message ($T_{\mathrm{SM3,digest}}$) is:

$$\left\{T_{\mathrm{SM3,digest}}\right\}_{\mathrm{ms}} \le \frac{240 \times 8}{6 \times 1024^2} \times 10^3 \approx 0.305 \tag{3}$$

The delays of signature ($T_{\mathrm{HMAC,S}}$) and authentication ($T_{\mathrm{HMAC,A}}$) are calculated, respectively, as (4) and (5).

$$\left\{T_{\mathrm{HMAC,S}}\right\}_{\mathrm{ms}} = \frac{10^3}{14705} \approx 0.068 \tag{4}$$

$$\left\{T_{\mathrm{HMAC,A}}\right\}_{\mathrm{ms}} = \frac{10^3}{7812} \approx 0.128 \tag{5}$$

Data transmitted during security operations of the GOOSE/SMV messages are the cryptographic key and the input and output data of the signature/authentication. The transmission rate of serial peripheral interface (SPI) of the A980 chip is 12 Mbit/s, so the transmission delay of GOOSE/SMV during the security operations ($T_{\mathrm{GOOSE/SMV,SPI}}$) is:

Table 2 Calculating speed of partial algorithms of A980 chip

Algorithm	SM2 (tps)	SM3 (Mbit/s)	AES (Mbit/s)	SHA256 (Mbit/s)	HMAC_SHA256 (tps)
Encryption	112	–	9	–	–
Decryption	119	–	7	–	–
Signature	285	–	–	–	7812
Authentication	101	–	–	–	14705
Digest calculation	–	6	–	4	–

STATE GRID
STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

$$\left\{T_{\mathrm{GOOSE/SMV,SPI}}\right\}_{\mathrm{ms}}=\frac{2\times(240\times 8+800+256)\times 10^3}{12\times 1024^2}\approx 0.473 \tag{6}$$

Therefore, the security operation delay of GOOSE/SMV message ($T_{\mathrm{GOOSE/SMV,Sec}}$) is:

$$T_{\mathrm{GOOSE/SMV,\,Sec}}=2T_{\mathrm{SM3,digest}}+T_{\mathrm{HMAC,S}}+T_{\mathrm{HMAC,A}}+T_{\mathrm{GOOSE/SMV,SPI}}\approx 1.279\ \mathrm{ms} \tag{7}$$

4.2.2 Analysis for security operation delay of MMS

According to Fig. 4, the delay of the security operation of the MMS message comes from the following processes: the digest calculation, the signature and authentication of the time field, and the encryption and decryption of the MMS message. The length of the time field is generally no more than 4 bytes and the time of digest calculation is about 0.001 ms, so the delay of digest calculation is negligible.

The delay of completing a process of the signature ($T_{\mathrm{SM2,S}}$) and authentication ($T_{\mathrm{SM2,A}}$) is:

$$\left\{T_{\mathrm{SM2,S}}+T_{\mathrm{SM2,A}}\right\}_{\mathrm{ms}}=\frac{10^3}{285}+\frac{10^3}{101}\approx 13.4 \tag{8}$$

The length of the signature generated by the SM2 algorithm is 512 bits. Without encryption, data to be transmitted during security operations include the time field and signature field, so the transmission delay during security operations ($T_{\mathrm{MMS1,SPI}}$) is:

$$\left\{T_{\mathrm{MMS1,SPI}}\right\}_{\mathrm{ms}}=\frac{(32+512)\times 2}{6\times 1024^2}\times 10^3\approx 0.173 \tag{9}$$

Therefore, without encryption, the security operations delay of MMS ($T_{\mathrm{MMS1,Sec}}$) is calculated as:

$$T_{\mathrm{MMS1,Sec}}=T_{\mathrm{SM2,S}}+T_{\mathrm{SM2,A}}+T_{\mathrm{MMS1,SPI}}\approx 3.573\ \mathrm{ms} \tag{10}$$

In addition, the delay of completing a process of encryption ($T_{\mathrm{SM2,E}}$) and decryption ($T_{\mathrm{SM2,D}}$) is:

$$\left\{T_{\mathrm{SM2,E}}+T_{\mathrm{SM2,D}}\right\}_{\mathrm{ms}}=\frac{10^3}{112}+\frac{10^3}{119}\approx 17.3 \tag{11}$$

Date encrypted by SM2 include two BigInteger (x and y), hash value and ciphertext. The length of x, y or hash value is 256 bits, and the length of ciphertext is equal to the length of plaintext. When MMS messages adopt the method of signature-then-encryption on the sending side and decryption-then-authentication on the receiving side, the transmitted data during security operations include plaintext, x, y, hash value and ciphertext. So the transmission delay during security operations ($T_{\mathrm{MMS2,SPI}}$) is:

$$\left\{T_{\mathrm{MMS2,SPI}}\right\}_{\mathrm{ms}}=\frac{(256\times 2+32\times 3)\times 8\times 2}{12\times 1024^2}\times 10^3\approx 0.928 \tag{12}$$

Therefore, when encryption is adopted, the security delay of operations of MMS ($T_{\mathrm{MMS2,sec}}$) is:

$$T_{\mathrm{MMS2,Sec}}=T_{\mathrm{SM2,S}}+T_{\mathrm{SM2,A}}+T_{\mathrm{SM2,E}}+T_{\mathrm{SM2,D}}+T_{\mathrm{MMS2,SPI}}=31.628\ \mathrm{ms} \tag{13}$$

4.2.3 Analysis for security operation delay of TLS

According to Fig. 8, delay of the security operations of the modified TLS primarily comes from the following processes:

1) Two digest calculations, two signature calculations and two authentication calculations in the process of mutual authentication.
2) In the client, the generation of the session key and its encryption by the server's public key before the receiver sends the ClientKeyExchange message.
3) The server uses its private key to decrypt the session key after receiving the ClientKeyExchange message.
4) The client or server calculates the digest of interacted handshake messages by the SHA256 algorithm, and carries out encryption or decryption of the digest by negotiated session key and cipher suites.

In the interaction process of TLS, the session key is calculated based on three random numbers generated by the server and client, which takes about 3 ms (T_{pk}). The length of the plaintext is 256 bits, which is the maximum plaintext length allowed by the SM2 signature algorithm. Therefore, the delay of mutual authentication ($T_{\mathrm{TLS,MA}}$) is:

$$\left\{T_{\mathrm{TLS,MA}}\right\}_{\mathrm{ms}}=\left(\frac{256}{4\times 10^3}+\frac{10^3}{285}+\frac{10^3}{101}\right)\times 2\approx 26.948 \tag{14}$$

Before and after transmitting the ClientKeyExchange message, the client and the server both adopt the SM2 algorithm to encrypt and decrypt the session key. The delay of this process is:

$$\left\{T_{\mathrm{TLS,SM2,E}}+T_{\mathrm{TLS,SM2,D}}\right\}_{\mathrm{ms}}=\frac{10^3}{112}+\frac{10^3}{119}\approx 17.3 \tag{15}$$

Except for the ChangeCipherSpec message, the length of the interacted message is 425 bytes, and the delay of its digest calculation with SHA256 ($T_{\mathrm{TLS,SHA256}}$) is:

$$\left\{T_{\mathrm{TLS,SHA256}}\right\}_{\mathrm{ms}}=\frac{425\times 8}{4\times 1024^2}\times 10^3\approx 0.811 \tag{16}$$

The delay of authentication with HMAC $T_{\mathrm{TLS,HMAC}}$ is:

$$\left\{T_{\mathrm{TLS,HMAC}}\right\}_{\mathrm{ms}}=\frac{10^3}{14705}+\frac{10^3}{7812}\approx 0.086 \tag{17}$$

The delay of encryption and decryption with ASE ($T_{\mathrm{TLS,AES}}$) is:

$$\left\{T_{\mathrm{TLS,AES}}\right\}_{\mathrm{ms}}=\left(\frac{256}{9\times 1024^2}+\frac{256}{7\times 1024^2}\right)\times 10^3\approx 0.062 \tag{18}$$

Data to be transmitted during the security operations of TLS include three plaintexts of 1024 bits, three signatures, two keys of 256 bits and a partial interacted message, which is a total of 905 bytes. The transmission delay between the security chip and master CPU ($T_{\mathrm{TLS,SPI}}$) is:

$$\left\{T_{\mathrm{TLS,SPI}}\right\}_{\mathrm{ms}}=\frac{905\times 8}{12\times 1024^2}\times 10^3\approx 0.575 \tag{19}$$

Therefore, the total delay of the TLS security operations ($T_{\mathrm{TLS,Sec}}$) is:

$$\begin{aligned}T_{\mathrm{TLS,Sec}}&=\left(T_{\mathrm{TLS,SHA256}}+T_{\mathrm{TLS,HMAC}}+T_{\mathrm{TLS,AES}}\right)\times 2+T_{\mathrm{pk}}\\&\quad+T_{\mathrm{TLS,SM2,E}}+T_{\mathrm{TLS,SM2,D}}+T_{\mathrm{TLS,MA}}+T_{\mathrm{TLS,SPI}}\\&=49.741\ \mathrm{ms}\end{aligned} \tag{20}$$

4.3 Simulation for delays of substation communications

To obtain T_{other} in (1) in addition to the security operation delay, we establish a substation network model of type D2-1 defined in IEC 61850-5 in the simulation software. The specific network structure of type D2-1 is given in [21]. This section will present the configuration and result of simulation for delays of the substation communications, including communications between two substations and communications within a substation.

4.3.1 Simulation for delays of communications within substation

Five typical data flows including sampled value message, trip message, switch status message, device status message and the file transfer message of the intelligent substations are simulated. After deploying security measures, the relevant parameters of the five flows are shown in Table 3.

In the simulation, we set MU to upload the sampled value message at $t = 0$. P&C starts to upload the device status message to the station server at $t = 3$ s. An error occurs at a bay at $t = 5$ s, P&C IED sends a tripping message to the circuit breaker, and then the circuit breaker returns a switch status message to P&C IED. The file is transmitted during 6–7 s. The result of the simulation is shown in Fig. 10.

Figure 10 shows that the average delay of the network in the substations is 0.135 ms. When a server sends file transfer messages to the host, the average delay increases to 0.24 ms. After the file transfer, the average delay is stable at 0.135 ms. The delay of the GOOSE/SMV messages is about 0.13 ms and the delay of device status messages is 0.22 ms. The maximum delay of the file transfer message is 0.5 ms.

4.3.2 Simulation for delays of telecontrol communications

The authentication based on the challenge-response mechanism will delay for about 120 s after one authentication, so it can be considered that the mechanism does not affect the real-time performance of communication services. Therefore, the delay of the challenge-response authentication mechanism is ignored in the analysis, and we primarily simulate the telecontrol communications

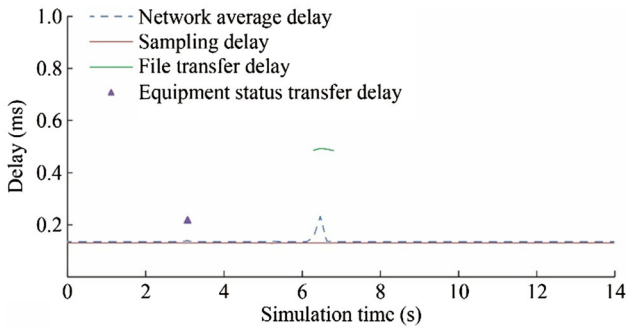

Fig. 10 Simulation result of communication delays within substation

Table 3 Parameters of the five data flows for simulation

Data flow	Message	Transmission direction	Period (ms)	Length of modified messages (byte)
Sampled value	SMV	MU→P&C	0.25	191
Trip	GOOSE	P&C→Breaker	Paroxysmal	145
Switch status	GOOSE	Breaker→P&C	Paroxysmal	288
Device status	MMS	P&C→Server	30000	384
File transfer	MMS	Server→Station host	300000	1024^2

STATE GRID
STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

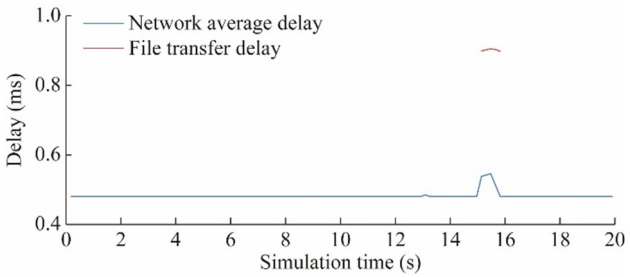

Fig. 11 Simulation result of delays for telecontrol communications

Table 4 Delays of secured communications and their requirements

Data flow	Delay requirement in IEC 61850 (ms)	Delay (ms)
Sampled value	< 3	1.409
Trip	< 3	1.409
Switch status	< 3	1.409
Device status	< 100	31.848
File transfer	500–1000	≤ 64.492

based on the modified TLS. It should be noted that, in addition to the communication delays by the simulation, a delay of T_{SDH} = 0.15 ms occurs when a message passes through a board on the SDH link.

The TLS handshake is set to start at t = 13 s and the larger file is transferred during 15–16 s, and the simulation result is shown in Fig. 11. The average delay is maintained at 0.481 ms. When the TLS handshake is carried out, the average delay increases to 0.496 ms. When the file transfer message is being transmitted, the average delay increases to 0.546 ms. After the file transferring stops, the average delay stabilizes at 0.488 ms. The maximum delay of the file transfer message is 0.878 ms.

4.4 End-to-end delay of secured communications

According to (1), the end-to-end delay of a communication employing the security measures of the proposed scheme can be obtained by summing up the above theoretical calculation results and simulation results, as shown in (22) to (24):

$$T_{GOOSE/SMV} = T_{GOOSE/SMV,Sec} + T_{GOOSE/SMV,other} = 1.409 \text{ ms} \quad (21)$$

$$T_{MMS} = T_{MMS2,Sec} + T_{MMS,other} = 31.848 \text{ ms} \quad (22)$$

$$T_{File} = T_{MMS1,Sec} + T_{TLS,Sec} + T_{FTP,other} = 63.820 \text{ ms} \quad (23)$$

$$T_{FarFile} = T_{MMS1,Sec} + T_{TLS,Sec} + T_{FarFile,other} + T_{SDH} = 64.492 \text{ ms} \quad (24)$$

where T_{File} is the end-to-end delay of file transfer inner substation; $T_{FarFile}$ is the end-to-end delay of telecontrol file transfer; $T_{GOOSE/SMV,other}$, $T_{MMS,other}$, $T_{FTP,other}$ and $T_{FarFile,other}$ are the delays in addition to security operations delay as (2).

The delay requirements specified in IEC 61850-5 [22] of the five data flows and their delays in the secured substation network are presented by Table 4, which shows that the end-to-end delays of secured communications based on the security scheme proposed in this paper meet the real-time requirements defined in IEC 61850-5 for intelligent substations.

To compare the proposed scheme in this paper with the existing works [5–8] in terms of real-time performance, the security operations in each scheme are listed in Table 5. Calculating the exact communication delay involves the work of selecting an encryption chip for each scheme, so it is not carried out in this paper. In Table 5, H is a hash operation, E is an encryption operation, D is a decryption operation, S is a signature operation, V is a verification operation, C is a certification operation, and N is a nonlinear operation.

The unit security strength of the elliptic curves cryptography (ECC) algorithm is higher than the RSA algorithm. Compared with RSA, ECC has advantages in terms of memory usage, resource consumption and encryption speed [23]. Therefore, according to Table 5, it can be concluded that our scheme is better than existing works in

Table 5 Comparison of security operations between existing work and this paper in real-time performance

Source	Security operations		
	GOOSE/SMV	MMS	TLS
[5]	$2E + 2D + 2N$	–	–
[6]	$2H_{SM3} + S_{SM2} + V_{SM2} + 2C$	–	–
[7]	–	–	$2S_{SM2} + 2V_{SM2} + 2C + E_{RSA} + D_{RSA} + E_{SM4} + D_{SM4} + 4H_{SM3}$
[8]	$E_{RSA} + D_{RSA} + E_{DES} + D_{DES}$	–	–
This paper	$2H_{SM3} + S_{HMAC} + D_{HMAC}$	$S_{SM2} + V_{SM2} + E_{SM2} + D_{SM2}$	$2H_{SM3} + 2S_{SM2} + 2V_{SM2} + E_{SM2} + D_{SM2} + E_{ASE} + D_{ASE} + 2H_{256}$

real-time performance under the same computing performance.

5 Conclusion

It is urgent to deploy security measures for intelligent substation communications. For this reason, the IEC has developed IEC 62351, but it has shortcomings for real-time performance and security capability, and offers no solution for the management of keys and certificates. In this paper, a new security scheme including security measures and a key management method is proposed for smart substations, which not only meets the security demands but also satisfies the real-time requirements of the communications. Considering the characteristics of a power system, we innovatively propose to employ CLPKC in an intelligent substation. This work provides a practical solution for securing the communications in intelligent substations and can be a reference for a revision of IEC 62351.

Acknowledgements This work is supported by the National Key Research and Development Program of China (No. 2017YFB0903000), the National Natural Science Foundation of China (No. 51377122) and the project of State Grid Corporation of China (Research on Cooperative Situation Awareness and Active Defense Method of Cyber Physical Power System for Cyber Attack).

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

[1] Cleveland F (2006) IEC TC57 security standards for the power system's information infrastructure. In: Proceedings of IEEE PES transmission and distribution conference and exhibition, Dallas, USA, 21–24 May 2006, pp 1079–1087
[2] Tong XY, Wang XR (2016) Inference and countermeasure presupposition of network attack in incident on Ukrainian power grid. Autom Electr Power Syst 40(7):144–148
[3] IEC 62351 (2005) Data and communications security
[4] Strobel M, Wiedermann N, Eckert C (2016) Novel weaknesses in IEC 62351 protected smart grid control systems. In: Proceedings of IEEE international conference on smart grid communications, Sydney, Australia, 6–9 November 2016, pp 266–270
[5] Wang B, Wang M, Zhang S (2013) A secure message transmission method based on GCM for smart substation. Autom Electr Power Syst 37(3):87–92
[6] Li L, Zhu Y (2009) Authentication scheme for substation information security based on chaotic theory. In: Proceedings of 2009 Asia-Pacific power and energy engineering conference, Wuhan, China, 28–31 March 2009, pp 1–3
[7] Luo Z, Xie JH, GU W et al (2015) Application of SM2 encrypted system in smart substation inner communication. Autom Electr Power Syst 39(13):116–123
[8] Zhao L, Yan T, ZHU JP et al (2016) Application of SM2 encrypted system in telecontrol communication for smart substation. Autom Electr Power Syst 40(19):127–133
[9] Wang FF, Wang HZ, Chen DQ et al (2014) Substation communication security research based on hybrid encryption of DES and RSA. In: Proceedings of 9th international conference on intelligent information hiding and multimedia signal processing, Beijing, China, 16–18 October 2014, pp 437–441
[10] Suhendray V, Wu YD, Saputra H et al (2016) Lightweight key management protocols for smart grids. In: Proceedings of IEEE international conference on internet of things, Chengdu, China, 15–18 December 2016, pp 345–348
[11] He XZ, Pun MO, Jay Kuo CC (2012) Secure and efficient cryptosystem for smart grid using homomorphic encryption. In: Proceedings of IEEE power and energy society innovative smart grid technologies, Washington DC, USA, 16–20 January 2012, pp 1–8
[12] Nicanfar H, Jokar P, Beznosov K et al (2014) Efficient authentication and key management mechanisms for smart grid communications. IEEE Syst J 8(2):629–640
[13] Fuloria S, Anderson R, Mcgrath K et al (2010) The protection of substation communications. http://101.96.10.42/pdfs.semanticscholar.org/5970/094d87e87f94e73494523116ba24cfcec584.pdf. Accessed 2 May 2016
[14] Cui XH (2016) Research on the security of message and its real-time in smart substation. Dissertation, Harbin Institute of Technology
[15] Al-Riyami SS, Paterson KG (2003) Certificateless public key cryptography. In: Laih CS (ed) Advances in cryptology: ASIACRYPT 2003. Springer, Heidelberg, pp 452–473
[16] Dent AW (2008) A survey of certificateless encryption schemes and security models. Int J Info Secur 7(5):349–377
[17] Baek J, Safavi-Naini R, Susilo W (2005) Certificateless public key encryption without pairing. In: Zhou J, Lopez J, Deng RH et al (eds) Information security, vol 3650. Springer, Heidelberg, pp 134–148
[18] Sun YX, Zhang FT, Baek J (2007) Strongly secure certificateless public key encryption without pairing. In: Bao F, Ling S, Okamoto T et al (eds) Cryptology and network security, vol 4856. Springer, Heidelberg, pp 194–208
[19] Zhang FT, Sun YX, Zhang L et al (2011) Research on certificateless public key cryptography. J Softw 22(6):1316–1332
[20] Boneh D, Franklin M (2001) Identity-based encryption from the Weil pairing. In: Kilian J (ed) Advances in cryptology: CRYPTO 2001, vol 2139. Springer, Heidelberg, pp 213–229
[21] Zhang Z, Huang X, Cao Y et al (2011) Comprehensive data flow analysis and communication network simulation for virtual local area network-based substation. Power Syst Technol 35(5):204–209
[22] IEC 61850-5 (2003) Communication network and systems in substations—part 5: communication requirements for function and device models
[23] Zhan Y (2017) The comparison of RSA and ECC. https://blog.csdn.net/u010646653/article/details/73888734,2017-06-29. Accessed 28 December 2017

Jie ZHANG received the B.S. degree in computer science and technology from Shandong University, China. She is currently pursuing her master's degree in Wuhan University, China. Her research interest is communication security for power systems.

Jun'e LI is a professor in Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, China. Her research interests include computer network architecture, cyber security, and the security of cyber-physical systems.

Xiong CHEN is an engineer in NARI Group Corporation/State Grid Electric Power Research Institute. His research interests include safety and stability control of power system.

Ming NI is a principal expert for grid planning and the national experts of Thousand Talents Plan. His research interests include power system planning and power cyber-physical systems.

Ting WANG is currently pursuing her master's degree in Wuhan University. Her research interest is communication security for power systems.

Jianbo LUO is a senior engineer in NARI Group Corporation/State Grid Electric Power Research Institute. His research interests include safety and stability control of power system.