Hindawi
Scientific Programming
Volume 2021, Article ID 6650725, 11 pages
https://doi.org/10.1155/2021/6650725

*Research Article*

# Research on Distributed Feeder Automation Communication Based on XMPP and GOOSE

**Lingyan Sun**,[1] **Yu Chen**,[1] **Chuiyue Kong**,[1] **and Jinghua Wang**[2]

[1]*School of Electrical and Electronic Engineering, Shandong University of Technology, Zibo 255000, China*
[2]*Shandong Kehui Electric Automation Co., Ltd., Zibo 255000, China*

Correspondence should be addressed to Lingyan Sun; 591824299@qq.com and Yu Chen; chenyu@sdut.edu.cn

Received 7 October 2020; Revised 14 December 2020; Accepted 28 January 2021; Published 8 February 2021

Academic Editor: Ting Yang

In the application process of distributed feeder automation (FA) that is based on peer-to-peer exchange of measurement and control data between smart terminal units (STUs), there is an urgent need for standardized communication interaction and necessary security protection. This paper proposes an IEC 61850 communication mapping scheme using built-in secure extensible messaging and presence protocol (XMPP) and the generic object oriented substation event based on the user datagram protocol (GOOSE over UDP) and a security protection scheme based on hash to obtain random subsets (HORS); one-time signature algorithm is used to ensure the communication safety of GOOSE messages. The agent-based distributed FA test system is developed with the STUs. The test results show the scheme can meet the requirements of the quick distributed feeder automation.

## 1. Introduction

The structure of the distribution line is complex and the failure rate is high. At the same time, the requirements for power supply quality and reliability from users become stringent. The distributed feeder automation can effectively speed up the failure processing speed and improve the power supply reliability [1, 2]. The technology of distributed FA based on the peer-to-peer exchange of measurement and control data between STUs has attracted wide attention due to its comprehensive utilization of information, fast local control speed, and perfect performance. However, there are several issues to be solved in the existing FA system: (1) the private information model and communication mechanism are adopted in the information communication of STUs of various manufacturers, which lack the support of standard information model and communication mechanism, resulting in the failure to realize the interoperability of different STUs; (2) the communication between STUs lacks the unified service scheme and necessary security protection technology.

Distributed FA control is to realize fault handling through peer-to-peer communication between STUs, which requires a unified information model, communication mapping and reliable communication network. In terms of information model, at present, the information model of distribution network is mainly based on IEC 61850. In the work by Ling's team [3], the FA controller is used to realize the control of the terminal and the expansion and control of the logical node to complete the distributed FA control; chen's team [4] proposed a peer-to-peer communication data exchange method for GOOSE services and established proprietary logical node and smart distributed FA model. In terms of information model, new or expanded logical nodes are often used to meet the requirements of distributed FA. In terms of communication network, IP communication network is generally used and fiber-optic communication has become the first choice of distribution communication network due to its reliable performance and strong anti-interference ability. Data transmission is mostly realized by the method of communication mapping. At present, the research on communication transmission protocol mainly includes IEC 60870-5-101/104, MMS, Web Services, and GOOSE. Among them, MMS is mainly used in substation and Web Services cannot meet the requirements of real-time performance and security of distribution network, so there are few applications of distribution network. IEC 60870-5-

101/104 is the most widely used communication mapping protocol in distribution network. In order to ensure the security of communication information, when IEC 60870-5-101/104 protocol is applied in distribution network, China state grid requires encryption when control command is issued, but it only solves the issue of longitudinal security from master station to terminal and does not solve the lateral security from terminal to terminal. In order to solve the issue of communication security, the working group of IEC TC57 proposed XMPP communication mapping and is developing corresponding standards; Hussain's team [5] studied service mapping scheme for IEC 61850-based XMPP communication; Wang's team [6] optimized and improved the mapping scheme of XMPP and verified the simplicity and efficiency of the scheme to achieve interoperability among devices with limited resources in the Internet of Things. Cho's team [7] has built an XMPP platform based on the IEC 61850 of the Internet of Things, which can effectively monitor DER; Hou's team [8] studied the real-time communication of XMPP and verified that the communication delay time mapped from IEC 61850 to XMPP can meet the real-time performance requirements of master station and STUs in distribution automation, and the communication delay time between STUs can meet the real-time performance requirements of slow distributed FA but not the quick distributed FA. For the fast transmission technologies of real-time control data, GOOSE transmission mechanism is often used. In the work by Chen's team [9], the mapping scheme of existing GOOSE is introduced in detail, and the optimized GOOSE mapping method based on TCP protocol is proposed. In the work by Fan's team [10], the existing GOOSE mapping is analyzed based on the requirements of distributed control communication, and the mapping scheme of GOOSE over UDP is proposed. Chen and Fan et al. have verified through experiments that the real-time performance of the GOOSE mechanism can meet the requirements of distributed control [9, 10]. The above studies have solved the cross-communication network issue when GOOSE transmission is used in the distribution network, but none of them considers the security protection of GOOSE transmission.

In order to realize the interoperability between the STUs of the distributed FA in the distribution network and effectively solve the issue about communication security, this paper studies the solution based on the combination of XMPP and GOOSE over UDP, the XMPP protocol mapping is used to realize the transmission of conventional data, and GOOSE over UDP is used to realize the transmission of real-time control data (such as switch action and protection trip). A one-time signature algorithm is used to solve the security protection issue of the GOOSE mechanism, and the real-time performance of the proposed transmission scheme is tested on the constructed platform.

## 2. Distributed FA

The distributed FA system is composed of master station of distribution automation system, STUs, and peer-to-peer communication network. Its main functions are as follows: (1) when the system is in normal operation, the STUs monitors the corresponding primary switchgear status information and reports it to the master station; (2) when a fault occurs on the system, peer-to-peer real-time interactive data between STUs realize fault location, isolation, and service restoration, that is, FLISR function, and report the processing results to the master station.

When a short-circuit fault occurs on the distribution lines, the outlet circuit breaker and related STUs detect the fault current. The circuit breaker trips to re-move the fault, and the STU that detects the fault current starts the FA function and judge the fault section according to whether there is fault current flowing through adjacent switches. In Figure 1, because STU0 and STU1, respectively, detect that there is fault current flowing at CB1 and switch S1, it is judged that the fault does not occur in the adjacent section of CB1. STU2 detects that there is no fault current at switch S2 of the switch adjacent to switch S1 and judges that the fault occurs in the section where K1 point is located. After determining the fault section, STU participating in decision control runs FLISR algorithm to generate fault isolation and recovery scheme. STU1 and STU2 execute the command to disconnect switch S1 and switch S2, respectively, isolate the fault section, and send the confirmation message. STU3 and STU0 execute command to close contact switch S3 and circuit breaker CB1 successively to re-store power supply.

If the distribution lines include distributed energy resource (DER), as the access of DER changes the structure of the distribution network and changes in electrical quantities, it is necessary to locate the fault based on the comparison of the magnitude of the fault current or the phase comparison [11].

According to the number of STU involved in decision-making control, the implementation mode of distributed FA can be divided into cooperative mode distributed FA and agent mode distributed FA [8].

*2.1. Cooperative Mode Distributed FA.* Cooperative mode distributed FA refers to two or more STUs to jointly participate in decision-making to realize the function of distributed FLISR. When a fault occurs on distribution lines, STU which detects fault information of field switch starts FA function, exchanges information with adjacent STU and runs FLISR algorithm, makes logical judgments independently, and determines the fault section. After generating the fault isolation recovery scheme, each STU sends the sequence control command locally, and the corresponding switch executes the action to realize FLISR operation.

*2.2. Agent Mode Distributed FA.* The agent mode distributed FA is a decision-making control that a designated STU completes the FLISR function. Generally, the STU at the outlet power switch of the substation is selected as the agent STU by taking the feeder as the unit, and the other STU are collectively referred to as the slave STU. Each STU in the ring network transmits the detected information to the corresponding agent STU. The agent STU initiates the logic of fault handling and decides the switch action and transmits the control command to the corresponding slave STU. In

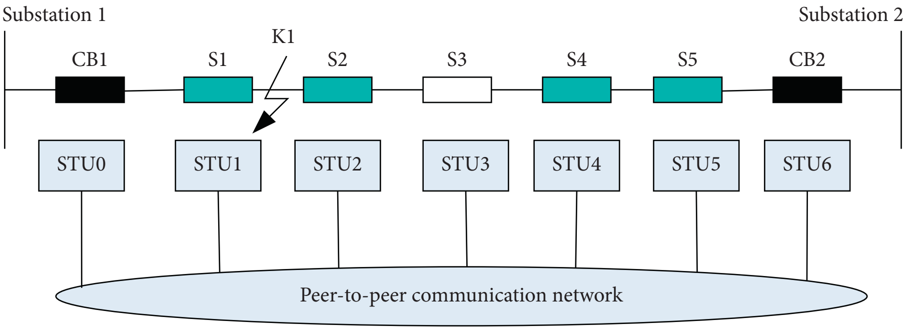


FIGURE 1: A distributed FA system for an open loop overhead line.

this mode, the principle of distributed FA is similar to centralized FA [8], in which the agent STU is equivalent to the substation of distribution network.

*2.3. Real-Time Performance Requirements of Distributed FA.* Distributed FA can effectively speed up the processing speed of distribution lines faults and reduce the outage time. According to different load types and communication conditions, it can be divided into quick distributed FA and slow distributed FA. The China national standard GB/T 35732-2017, Technical Specifications of Intelligent Remote Terminal Unit of Distribution Automation [12] specifies the information interaction and fault processing time, as shown in Table 1.

*2.4. Communication Security Requirements of Distributed FA.* In recent years, network security incidents occur frequently. In 2015, Ukraine, and in 2016, Israel, suffered hacker attacks on the power system, resulting in power outage. This indicates that the risk of grid network and information security exists for a long time and needs to be effectively protected.

In the distributed FA system, the data interaction object is mainly the STU and the master station. The STUs are distributed outdoors and scattered in a broad area in distribution automation system. Most of the environments are unattended and vulnerable to attack. The content of data interaction involves real-time measured current and voltage information, fault indication, switch position, control commands, etc. and its operation object is directly oriented to sectionalising switches. If the STUs are attacked or the interactive data are leaked or tampered and the wrong instructions are conveyed, the circuit outage and other accidents will occur directly.

Technical report IEC 61850 90-5 is used in the wide area phase angle measurement application in combination with communication security standard IEC 62351, and the method of establishing key distribution center (KDC) signature authentication is used for security protection. This method is more suitable for agent mode distributed FA, when applied to cooperative mode distributed FA, the number of key required is large, and the management is complex. In addition, The STU as the KDC is limited due to its computational ability, the key cannot be too long, and the security protection capability is limited.

At present, for the security protection of distribution network, China state grid clearly states that the security protection must be done according to the following requirements: the master station in distribution automation system should meet the one-way authentication function of nonsymmetric encryption key technology, and the STUs should have the function of authenticating the digital signature of the master station, but it only involves the security protection between the STUs and the master station; it does not require the security issues between the STUs. At the same time, it needs to strengthen the safety monitoring and management of the STUs and other equipment. Electrical Internet of Things also puts forward requirements for grid security: eliminate the weak links in the grid, use new technologies or new methods to improve the security protection of important equipment and time periods in the grid, and strengthen the security prevention and control of important information transmission to prevent the impact of "network attack" on the grid.

In the current IEC 61850 communication protocol, XMPP can support various kinds of security encryption algorithms, so in this paper, XMPP mapping communication is used for information model and measurement data, and GOOSE over UDP is used for real-time control command; at the same time, security protection is added to it.

## 3. Communication Mapping of XMPP in Distributed FA

*3.1. XMPP Working Mechanism.* XMPP is an open-source communication protocol for real-time communication. It is based on extensible markup language (XML), which can meet the needs of thousands of STUs online and interconnected at the same time. XMPP protocol has been standardized by Internet Engineering working group, and core protocols (such as RFC 6120, RFC 6121, and RFC 6122) have been released and updated. XMPP core specification has built-in relatively sound security mechanism. The IEC 61850 8-2 standard which is being developed by IEC TC57 organization adopts the XMPP mapping method to solve the network security issue.

As shown in Figure 2, XMPP supports mode applications of client/server (C/S) and server/server (S/S) and can also communicate with external networks through gateways.

Table 1: Technical requirements for distributed FA.

| Types of distributed FA | Information interaction time (ms) | Fault upstream switch isolation time (ms) | Recovery time of nonfault area (s) | Signal up time (s) |
|---|---|---|---|---|
| Quick distributed FA | ≤20 | ≤200 | ≤5 | ≤3 |
| Slow distributed FA | ≤200 | ≤5000 | ≤45 | ≤3 |

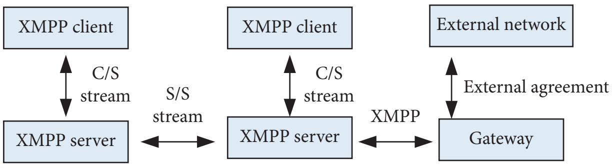


Figure 2: Typical network architecture of XMPP.

Communication between XMPP clients needs to be connected with XMPP server and forwarded by XMPP server:

(1) The client establishes a connection with the server through TCP/IP and optionally sets the encryption option of transport layer security (TLS) to ensure the security of transport flow information

(2) The client and server use simple authentication security layer (SASL) to obtain identity authentication

(3) Open the XML stream and bind the client resources to form a complete identification JID (Jabber ID)

(4) The client makes the JID of target address, and after the server looks up and authentication, a session between clients is establish. The specific message fragments are encapsulated in the middle of the stream in the form of XML stanza and transmitted in the form of XML stream. XMPP defines three different XML stanza-<iq/>, <presence/>, <message/>, to achieve different functions.

*3.2. Distributed FA System Architecture Based on XMPP Mapping.* The distributed FA system applies XMPP, as shown in Figure 3. STUs can be used as both the IEC 61850 client and the IEC 61850 server, but both of them are XMPP clients for XMPP communication. They need to be connected to the XMPP server set up in the communication network through TCP/IP protocol, and the server will transmit them to realize the conversation between clients. The configuration of the server can be selected according to the size of the system and the light and heavy load the server bears, for example:

(1) Set up a single server in the master station or run XMPP server application in the front-end processor

(2) Subregional settings, such as configure the server by feeder group

Cooperative mode distributed FA and agent mode distributed FA differ in the number of STUs participating in decision-making control, resulting in different data flow and data transmission volume. When a fault occurs on distribution lines, the data transmission capacity of collaborative mode distributed FA and agent mode distributed FA is similar in fault isolation and recovery. However, during fault location, because collaborative distributed FA requires adjacent STUs for two-way interaction, there are many times of forwarding through the server and the server processes a large amount of information. The agent mode distributed FA only needs to be transmitted from the slave STU to the agent STU, and there is less interactive data forwarding. The real-time performance of the agent mode distributed FA is better than that of the collaborative distributed FA.

*3.3. Service Mapping of XMPP.* When XMPP is used for data transmission, the size of common data packets is usually several thousand bytes; since it has been transferred, encrypted, and decrypted through XMPP server, the actual transmission delay may be large in case of network blocking or large data packets; in this paper, XMPP is not used to transmit real-time control data with high real-time performance requirements; XMPP is used to transmit nonfault information model data, real-time measurement data, and historical data. The data are encapsulated in the XML stream in the form of XML stanza. After establishing the TCP/IP link, through the forwarding of the XMPP server, XML stream transmission from the STU to the STU is completed. The types of XML message format include <iq/>, <message/> and <presence/>.

When XMPP is used for information model data mapping, the most commonly used information exchange models are DataSet, Report, and Log. Among them, DataSet defines data values and data attribute values of logical nodes, and when the Report monitors that the information changes, that is to say, when the trigger condition is reached, the Report will immediately send the data set members to the client, and the whole process is recorded by Log; when the real-time measurement data and historical data are transmitted, the client completes the data transmission from the client to the client by forwarding the data set through the server in the XML stream. The association established before mapping uses two party application association of end-to-end information flow control.

Abstract communication service interface (ACSI) has no communication function and does not specify specific message format and encoding/decoding syntax [13]; therefore, IEC 61850 maps the information model and services of ACSI to specific communication service mapping (such as MMS and XMPP), in which MMS uses ASN.1 to make corresponding format regulations for service coding, and the coding format is BER, while XMPP mapping also uses similar data unit structure, but the coding mode is XER, and the specific mapping relationship is shown in Table 2.

*3.4. Safety Protection of XMPP.* Distributed FA uses XMPP for data transmission, mainly in the form of XML stream between the master station and the STUs or between the

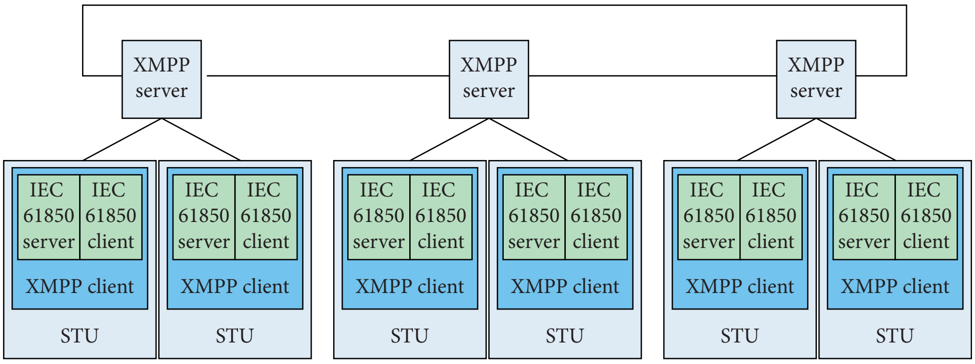


Figure 3: The architecture of XMPP in distributed FA systems.

Table 2: Distributed feeder automation related ACSI mapping table.

| IEC 61850 object | ACSIe service | ASN.1 BER of MMS | XML stanza and type of XMPP |
|---|---|---|---|
| Associate | Associate | Initate-requestPDU<br>Initate-responsePDU<br>Initate-errorPDU | IQ Type-set<br>IQ Type-result<br>IQ Type-result |
| Data | GetDataValues | Read-requestPDU<br>Read-responsePDU | IQ Type-get<br>IQ Type-result |
| | SetDataValues | Write-requestPDU<br>Write-responsePDU | IQ Type-set<br>IQ Type-result |
| | GetDataDefinition | GetVariableAccessAttrbute-requestPDU<br>GetVariableAccessAttrbute-responsePDU | IQ Type-get<br>IQ Type-result |
| Report | Report | InformationReport-requestPDU | Message Type-normal |
| | GetBRCBValues | Read-requestPDU<br>Read-responsePDU | IQ Type-get<br>IQ Type-result |
| | SetBRCBValues | Write-requestPDU<br>Write-responsePDU | IQ Type-set<br>IQ Type-result |
| Control | Operate | Write-requestPDU<br>Write-responsePDU | IQ Type-set<br>IQ Type-result |
| LCB | SetLCBValues | Write-requestPDU<br>Write-responsePDU | IQ Type-set<br>IQ Type-result |
| File | SetFile | ObtainFile-requestPDU<br>ObtainFile-responsePDU | IQ type-get<br>IQ Type-result |
| Data set | GetDataSetValues | Read-requestPDU<br>Read-responsePDU | IQ Type-get<br>IQ Type-result |
| | SetDataSetValues | Write-requestPDU<br>Write-responsePDU | IQ Type-set<br>IQ Type-result |

STU and the STU. During the transmission process, it may be subject to external malicious tampering, so this process needs effective security protection. XMPP itself contains two security mechanisms of transport layer security (TLS) and simple authentication security layer (SASL). Among them, TLS is used to encrypt the communication channel to ensure the information security of the data flow from the client to the server or from the server to the server; SASL is used to authorize the user, and multiple authentication mechanisms are included to ensure the safety of the transmission of information.

XMPP has two built-in security mechanisms; among them, TLS is divided into two layers. The three protocols of handshake, password specification change, and alarm contained in the upper layer, respectively, have the functions of identity authentication, security parameter negotiation and change notification, flow closing, and error alarm, which can ensure the security of communication; the lower record layer protocol can encrypt and decrypt data, decompress and compress data, and check data integrity to ensure data security; it uses STARTTLS extension. The sender sends <starttls/>command to indicate the start of STARTTLS negotiation. The receiver uses <processed/> or <failure/> to reply.

Since authentication information needs to be sent during SASL negotiation, STARTTLS negotiation needs to be completed before SASL negotiation; SASL provides GSSAP, DIGEST-MD5, SCRAM (SCRAM-SHA-1 and SASL-SCRAM-SHA-1-PLUS), PLAIN and other mechanisms to realize authentication. In distributed FA, authentication between STU and STU or between STU and master station is realized by SASL built-in XMPP, and the security of transmitted data is protected by TLS lower layer, identity authentication and error alarm are realized by TLS upper layer, and the security of data transmission is realized by XMPP built-in security protection.

## 4. Security Protection Scheme of GOOSE for Real-Time Data Transmission

In the distributed FA, this paper uses GOOSE to complete the transmission of fast real-time data. In order to realize the fast transmission of the message in the IP layer, the way of GOOSE over UDP is adopted, and it has the characteristics of based on peer-to-peer communication, fewer protocol control options, short message delay time, and fast transmission speed. At the same time, it meets the real-time performance requirements of distributed FA for control commands.

*4.1. The Information Transmission of GOOSE over UDP.* GOOSE over UDP adopts the publisher/subscriber mechanism. In order to ensure the data of real-time performance, priority is set in the Type of Service (TOS) field of the IP protocol in the network layer. TOS is considered to be composed of differentiated service code point (DSCP) and explicit congestion notification (ECN); in order to ensure the reliability of the data, the fast multiple retransmissions mechanism is adopted. At the same time, whether the message is lost or whether the communication is interrupted can be judged according to the allowable lifetime of the message. According to the status number (StNum) and the sequence number (SqNum), it can be judged whether the transmitted message has frame loss, wrong sequence, or repetition, and for more important information (such as switch action), double frame receiving mechanism is adopted to ensure the reliability of transmission information.

When using GOOSE transmission mechanism to realize FLISR function, such as agent mode distributed FA, multicast application association is adopted for communication, fault indication DataSet is sent to service restoration controller (SRC) through Report service for fault section judgment, and SRC completes fault isolation and recovery of nonfault section through Operate service [14].

*4.2. The Security Protection of GOOSE over UDP.* Distributed FA is used for fault handling, which has high requirements for the real-time performance, reliability, and safety of transmission messages. In order to ensure that the distributed FA can quickly and accurately implement the FLISR function, effective security protection is required for GOOSE messages.

In order to solve the security issue of GOOSE communication in substation, IEC 62351 recommends the authentication algorithm based on message authentication code (MAC). The MAC shall be generated through the computation of a 32 bit FCS calculated by ISO/IEC 13239 (ISO HDLC). Message digest is signed by RSASSA-PKCS1-V1_5 algorithm specified by RFC 2437 to generate digital signature with security encryption. In the work by Farooq's team [15], the encryption algorithm in IEC 62351 standard is tested for the encryption and decryption performance of GOOSE data. The encryption and decryption time is 4.31 ms when the CPU is Intel i5-3210M, the main frequency is 2.5 GHz, and the GOOSE data packet is 256 bytes. At present, the CPU speed of distribution terminal is relatively low. Taking the STUs of Kehui's PZK-360H as an example, the main frequency of STUs is 454 MHz, and the encryption and decryption time is 24.303 ms after conversion according to the CPU speed. If the GOOSE data packet exceeds 256 bytes, the encryption and decryption time is longer. Therefore, the real-time performance does not meet the requirement that information interaction time is less than 20 ms in the fast distributed FA. In addition, the memory overhead of the encryption algorithm recommended by IEC 62351 is also large.

In order to solve the security issue of real-time control data in distributed FA, this paper uses the authentication of one-time signature based on HORS to enable GOOSE over UDP to detect whether the message is complete and whether it is intruded. The one-time signature is based on one-way function without trap gate, which has asymmetric secret information. At the same time, it has low requirements for hardware equipment, and it is fast in generating and verifying signature, which makes the one-time signature suitable for multicast authentication. GOOSE uses the one-time signature for the transmission of multicast data as shown in Figure 4.

SRC is used as key distribution center (KDC). KDC protocol based on RFC 3547 allows to support one-time signature algorithm. At the same time, in order to ensure that the key will not be stolen or tampered, KDC needs to update the key and refer to the handling method of the key in IEC 61850 90-5; the key update can be divided into two types: regular update and irregular update. The regular update is the update of the key under normal conditions, and the time is generally set as 30 min to 48 h. Because the computing power of STUs is relatively weak, the key length is relatively short. In order to ensure sufficient security, the maximum key lifetime is set as 30 min. The key generated by KDC is sent to each STU through UDP/IP multicast. After receiving the key, the STUs will save it. When using GOOSE for message transmission, it will be added to the message. The order of using the key is opposite to that of generating the key. The specific signature process is as follows [16–18]:

(1) Key generation: generate $t$ random $n$ bit strings $(s_1, s_2, \ldots, s_t)$, which form the private key $S_K$. The public key is then computed as $P_K = (v_1, v_2, \ldots, v_t)$, where $v_i = f(s_i)$ and $f$ is a one-way function.

(2) Singing: to sign a message $M$, let $h = H(M)$, where $H$ is a hash function. Split $h$ into $k$ substrings $(h_1, h_2, \ldots, h_k)$ of $\log_2 t$ bits each. Interpret each $h_j$ as an integer $i_j$. The signature of message $M$ can be expressed as $(s_{i_1}, s_{i_2}, \ldots, s_{i_k})$, $1 \leq j \leq k$.

(3) Verification: the recipient verifies the signature of the message $M$ sent by the sender, uses the method in (2) to calculate and generates $(s_{i_1}', s_{i_2}', \ldots, s_{i_k}')$, compares and verifies with the original signature, and check if $f(s_j') = v_{ij}$ holds.

Once the signature of message $M$ is generated, it cannot be changed, but the tamper can tamper with the message by

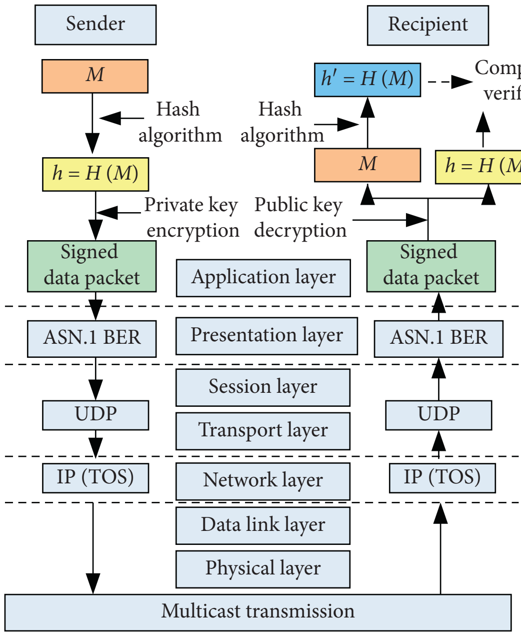


FIGURE 4: GOOSE multicast authentication data stream based on one-time signature.

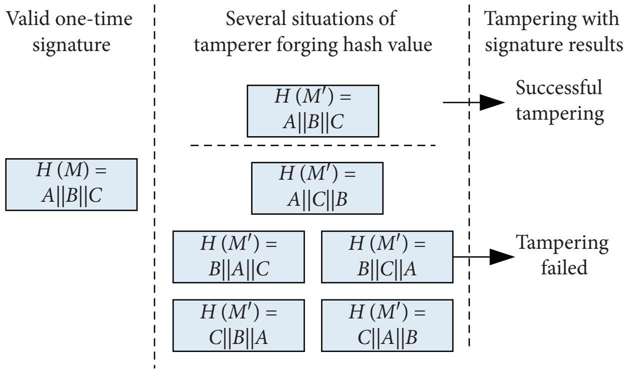


FIGURE 5: Tamperer forged signature case.

forging the same hash value as message $M$. Figure 5 shows the case of tampering with information when $k$ is taken as 3; the tamper changes message $M$ to $M'$, then we need to match the correct hash value from the $K$! Hash values, and so we can increase the security of one-time signature by increasing the size of $K$, but the calculation cost and signature size will also increase.

*4.3. The Influence of Distributed FA Control Mode on Message Encryption.* The control mode of distributed FA is divided into collaborative distributed FA and agent mode distributed FA. Because the STU of the cooperative mode distributed FA needs to communicate with the remaining $n-1$ STUs, and in order to ensure the security of the keys of STU, the STUs communicating with each other must contain keys that can only be identified by each other and KDC needs to send $n \times (n-1)$ keys. There is a large demand for the number of keys, a large amount of calculation and update work, and a high memory occupation of the STU; and the agent mode distributed FA takes the SRC as the KDC, SRC is responsible for managing and distributing the keys, and STU only needs to communicate with the SRC, so the number of keys is only $n$, and the number of keys is small. Considering the computing and storage capacity of the STU, agent mode distributed FA is more suitable for key distribution and management than collaborative distributed FA.

## 5. Experiment Test

The test is conducted for the agent mode distributed FA. The real-time control data between STUs and SRC are transmitted by GOOSE, and other data are transmitted by XMPP, as shown in Table 3.

*5.1. XMPP Message Test.* In order to test the real-time transmission performance of IEC 61850 information by XMPP, the communication test system as shown in Figure 6 is built, which is composed of optical Ethernet switch, router, PC, and relevant application software. PC1 installs the XMPP universal server Openfire. PC2PC7 are XMPP clients. The STU1 and STU2 are used for the XMPP data test. The STUs use Kehui's PZK-360H and built-in MPC 287 communication board with the main frequency of 454 MHz CPU, and the test program is developed in C++ under the embedded Linux operating system environment. PC4, PC5, PC6, and PC7 are used to simulate the other online users on the server in the distribution network, so as to realize the user login and the communication between the users, so as to generate the background traffic in the communication network. There are 502 simulated users in the test. The client program is implemented based on Java language, and the XMPP class library uses smack library.

The method of ping-pong test is adopted in communication delay test. First, record the time when STU1 sends a data packet as $t1$; STU2 receives the data packet from STU1, then sends it back to STU1, and records the time when STU1 receives the returned data packet as $t2$, and then the end-to-end data transmission delay is obtained by calculating the time difference between $t1$ and $t2$ divided by 2. Each message of different sizes sends 5000 packets. The measured end-to-end data transmission delay includes network transmission delay and server processing delay. Packets sent to the server need to wait in the packet queue processed by the server and be forwarded to the destination address by the server. If the transmitted data package is encrypted, because the key of different STUs are different, it needs to be decrypted first and then encrypted and forwarded in the XMPP server. Therefore, the processing delay of the XMPP server mainly includes the encryption and decryption delay of the server and the forwarding delay of the server.

It can be seen from Figure 7(a) that the communication message size has a great influence on the transmission delay, which basically shows that the transmission delay increases with the increase of the number of bytes in the message. The average delay of encryption with security is higher than that of encryption without security, mainly because of the encryption and decryption delay of the server. Based on XMPP to transmit IEC 61850 data objects, it is necessary to combine

Table 3: Communication content and security protection of distributed feeder automation.

| Communication object | Transmission mode | Transmission content | Safety protection |
|---|---|---|---|
| STU and SRC | GOOSE (fault) | Teleindication (signal of successful fault location, signal of successful switch disconnection, and signal of successful fault isolation)<br>Remote control (switch control command, etc.)<br>Telemetry (fault current value, etc.) | One-time signature |
|  | XMPP (nonfault) | Configuration, telemetry, teleindication | TLS and SASL |
| SRC and MS | XMPP | Configuration, telemetry, teleindication | TLS and SASL |
| STU and MS | XMPP | Configuration, telemetry, teleindication | TLS and SASL |

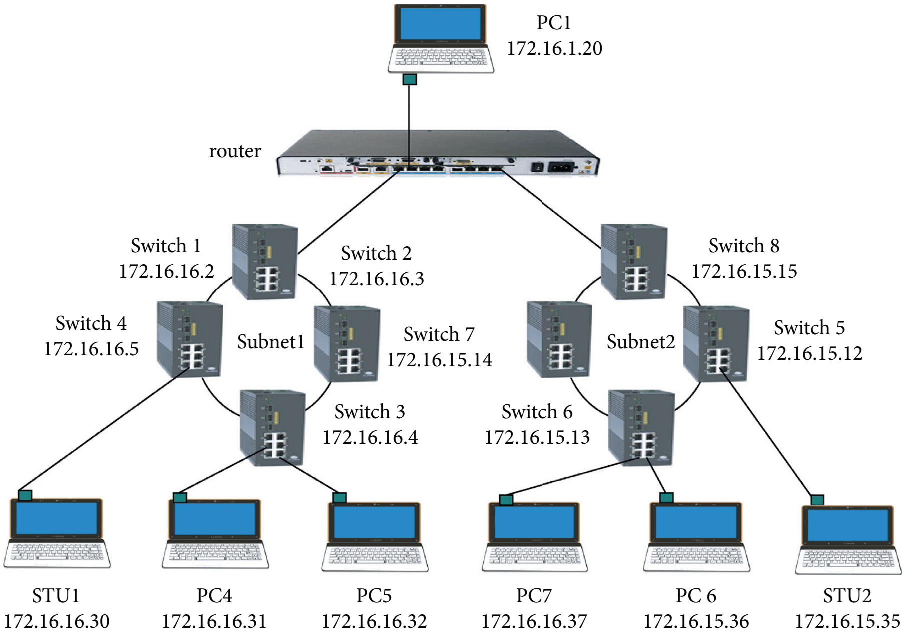
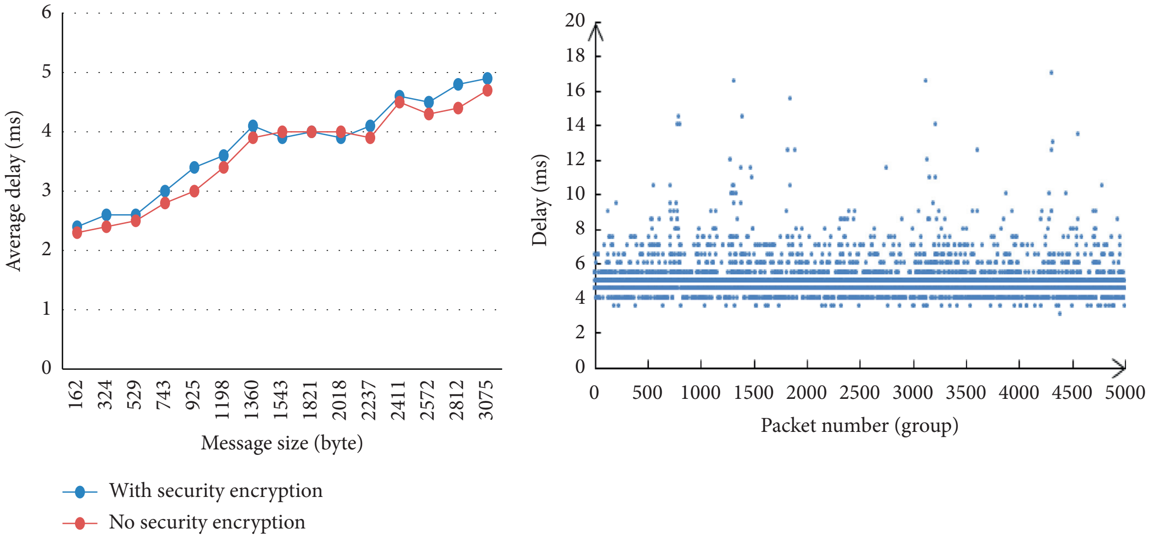


Figure 6: The test system of XMPP.



(a) (b)

Figure 7: XMPP transmission delay test: (a) end-to-end transmission delay of packet size; (b) the scatter plot of the transmission delay test with a packet size of 3075 bytes.

the data types and service parameters of IEC 61850 to expand based on XML to form multilayer definition tags to encapsulate data. Therefore, a typical XMPP encapsulated data packet is generally more than a few kilobytes. Taking 3075 bytes message as an example, the average end-to-end transmission delay based on XMPP with security encryption is about 4.9049 ms, and the maximum delay is about 17 ms. It can be seen from Figure 7(b) that the transmission delay under this message is mainly concentrated in 4–6 ms, and the large point of delay value is discontinuous.

The encryption delay of the message is tested on the PC with the CPU main frequency of 2.2 GHz, and the measured time is 0.3 ms. Converted to the STU using Blackfin as the processor and the main frequency of the main board as 300 MHz, its encryption delay is about 2.25 ms. Therefore, the transmission delay based on XMPP transmission from encrypting the sending end of the STU to receiving the message at the receiving end of the STU is about 7.5149 ms.

In the work by Fan's team [10], it is introduced that the distributed fast message of the distribution network is transmitted by GOOSE mechanism, and it is measured that the distributed measurement and control message based on GOOSE over UDP scheme is within 1.5 KB, and its transmission delay is within 2 ms. In contrast, XMPP-based distributed measurement and control messages have a relatively large transmission delay when the message is 1500 bytes, and the average delay is about 3.9 ms. The main reason is that XMPP packets need to be forwarded by the server to ensure security. In addition, because XMPP adopts XML plain text encoding form, when transmitting the same IEC 61850 information content, XMPP message is larger, so the delay is correspondingly increased.

The China National Standard [12] stipulates that the following: (1) the delay time of fault information interaction of peer-to-peer communication for fast distributed FA shall not be greater than 20 ms; (2) the delay time of fault information interaction message of peer-to-peer communication for slow distributed FA shall not be more than 200 ms. According to the test, the maximum end-to-end transmission delay of 3075 bytes' message during security encryption is 17 ms. But in actual application on-site, the size of XMPP data packet may be larger than 3000 bytes. Compared with the actual communication environment, the test network environment is stable and the server performance is better. Therefore, the maximum transmission delay of XMPP message in actual transmission may exceed 20 ms, but it meets the requirements of slow distributed FA for the transmission delay of information exchange, so it can be applied in slow distributed FA based on XMPP. It cannot meet the demand of fast distributed FA.

*5.2. The Real-Time Performance Test of GOOSE over UDP Message.* In order to test the real-time performance of using GOOSE over UDP to transmit control messages, a distributed FA test system is built as in Figure 8, the test platform is composed of the active static simulation platform of distribution network, communication network, STUs and PCs. The active static simulation platform of distribution network can simulate the failure of hand-held overhead line and cable line, and connect the voltage and current to the STUs through the corresponding transformer. The communication network consists of two SICOM3000 Ethernet switches, one router and single-mode optical fiber. The STUs uses five sets of PZK-360H from Kehui, and the PC is used to generate the background traffic in the network. In case of short-circuit fault of hand-held ring network, FLISR function is realized by GOOSE message communication between STUs. The time of fault isolation and recovery can be obtained by recording the trip contact signal output by the STUs and the fault simulation start contact signal time. Network message recording tool, Wireshark, is used to monitor the network and analysis GOOSE messages.

Since the STUs do not have the ability of high-precision time synchronization, it cannot directly test the transmission time of a single message between STUs. For the test of the transmission delay of GOOSE messages, the transmission delay can be realized by the ping-pong test (that is, the time difference between the sender's request message and the sender's acceptance of the response message divided by 2 as the transmission time) method after modifying the test program test.

The developed distributed FA test system uses the fault indication and control data set transmitted by GOOSE over UDP when a failure occurs; its message length is 335 bytes. Therefore, using the ping-pong method to test the GOOSE message transmission delay and encryption and decryption time are all for the 335 bytes GOOSE packet.

The failure test was carried out for the agent mode distributed FA, and the test was repeated 10 times, the signal of the switch node is recorded by the wave recorder to obtain the fault isolation time, and the log recorded in the STUs is used to obtain the encryption and decryption time, the fault detection time, and the switch control time. After the test, the total isolation time in agent mode distributed FA is 172.766 ms on average; among them, the average time from the over-current start to the protection information is written into the STU log as 17 ms. The average time from STUs receiving a remote control command to sending a remote control command to the switch is 19 ms, and the average time from STUs sending a remote control command to STUs detecting that the switch is off is 86 ms.

The encryption and decryption time of GOOSE message is shown in Table 4, and the average value of encryption and decryption time is 6.344 ms. The research group conducted a GOOSE over UDP transmission delay test with the message length of 335 bytes [10], and the average value of the transmission delay was 0.539 ms, so the transmission delay of the GOOSE messages with security encryption is about 6.883 ms. In Table 4, the transmission delay of STUs encryption is relatively smaller than that of decryption, because the separated message $M$ needs to be calculated using the hash algorithm when decrypting; and then the obtained digest $h'$ is compared with the original digest $h$ to verify the correctness of the signature. Encryption does not contain the separation and verification process, so the decryption time is slightly longer than the encryption time.

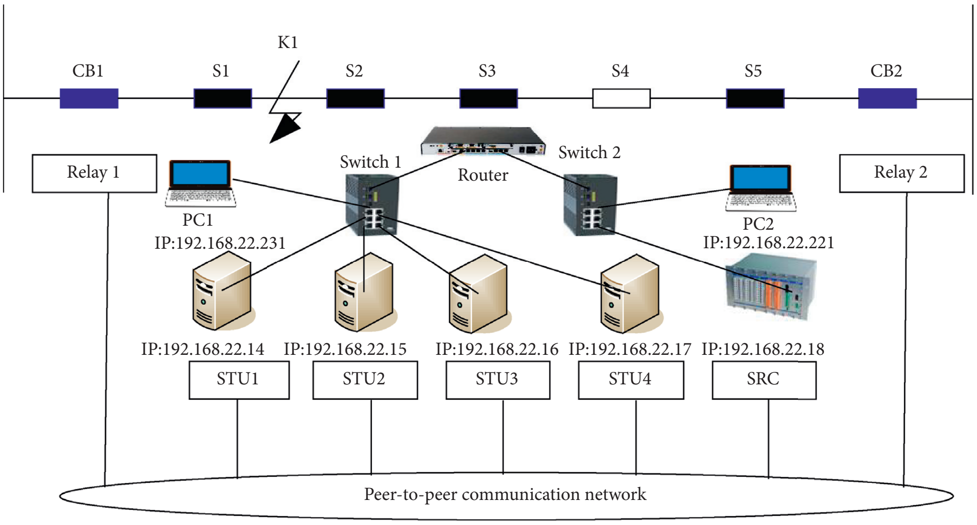


Figure 8: Distributed FA test system.

Table 4: Encryption and decryption time of GOOSE messages of STU.

| Encryption and decryption | Max. (ms) | Min. (ms) | Ave. (ms) |
|---|---|---|---|
| Encryption | 6 | 2 | 2.645 |
| Decryption | 7.125 | 2.809 | 3.699 |

For the transmission delay of GOOSE messages, it is not encrypted when the ping-pong method is used for testing, so as to reduce the processing delay of the STUs as much as possible. The test results are basically consistent with those of the work by Fan's team [10], which will not be discussed here.

PC2 is used to send data packets to PC1 to generate constant network background traffic, and different network load rates are generated by controlling the transmission rate. As shown in Figure 9, when the network load rate is less than 97%, the average transmission delay of the message is less than 7.3 ms and is less affected by the network background traffic, and when the network load rate is greater than 97%, the transmission delay increases sharply. In the distributed FA communication system of the distribution network, the network load rate generally does not exceed 30% [10], so the network load rate has little impact on the communication of the distributed FA.

In the process of distributed FA fault handling, real-time data are transmitted by GOOSE over UDP, and the Report after fault is transmitted to the master station through XMPP.

Based on the scheme developed in this paper, the average total isolation time of the test is 172.7 ms, which can basically meet the requirements of the fast distributed FA. In the total isolation time of distributed FA, the encryption and decryption time of GOOSE message and the communication delay of data packet account for a relatively small proportion. The main delay factors are fault detection and control strategy. Due to the need to transmit data to SRC for decision-making and then sending control commands to STUs for execution, the fault processing speed of agent mode distributed FA is slower than that of collaborative distributed FA, but the key distribution processing of agent mode distributed FA is easier than that of collaborative distributed FA.

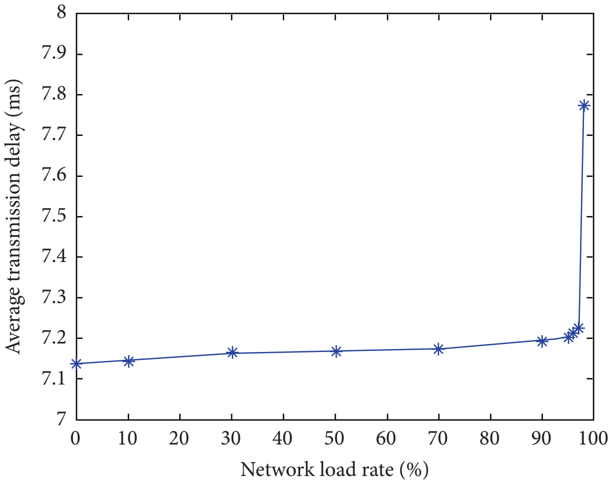


Figure 9: Transmission delay of different network load rates of GOOSE with secure encryption.

## 6. Summary

In order to standardize the communication mapping of distributed FA and solve the issue of communication security protection between STUs, this paper studies the IEC 61850 communication mapping issue of XMPP in the application of distributed FA. XMPP based on XML extension and built-in security mechanism can realize data encryption and integrity transmission. However, XMPP packets are transferred and encrypted in the server to a certain extent, which affects the real-time performance of transmission, and its real-time performance cannot meet the requirements of fast distributed FA. Realization of fast control data transmission through GOOSE over UDP can meet the real-time requirements of fast distributed FA. Due to the relatively weak computing capabilities of the STUs, the GOOSE message is protected by a one-time signature algorithm based on HORS with a small amount of calculation.

The test system is developed based on this scheme. The test results show that the transmission delay of XMPP can meet the requirements that the information interaction delay of slow distributed FA is no more than 200 ms, and the user authorization, authentication, and communication channel encryption technology based on SASL and TLS can realize the horizontal and vertical information security protection of distribution network, which provides a safe and effective communication mapping method for distributed control applications such as STUs and access of DERs. The real-time performance of GOOSE over UDP with increased security control can basically meet the requirements that the information interaction delay of fast distributed FA.

This paper conducts a preliminary study on the communication security of distributed FA; considering distribution and management for the key, the scheme is more suitable for the application of agent mode distributed FA. So, the agent mode distributed FA control is implemented at present, and the real-time performance is better when the collaborative distributed FA is adopted, but the management and distribution of the key are complicated. The next stage will further study the security control of the collaborative distributed FA.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

The work was supported by the Key Project of Smart Grid Technology and Equipment of National Key Research and Development Plan of China (No. 2016YFB0900600) and Technology Projects of State Grid Corporation of China (No. 52094017000W).

## References

[1] Y. Chen, Z. Zhu, B. Xu et al., “The use of IEC61850 for distribution automation,” in *Proceedings of the 2016 China International Conference on Electricity Distribution (CICED 2016)*, pp. 10–13, Xian, China, August 2016.

[2] T. Yip, J. Wang, B. Xu, K. Fan, and T. Li, “Fast self-healing control of faults in MV networks using distributed intelligence,” *CIRED-Open Access Proceedings Journal*, vol. 2017, no. 1, pp. 1131–1133, 2017.

[3] W. Ling, D. Liu, Y. Lu et al., “Model of intelligent distribution feeder automation based on IEC 61850,” *Automation of Electric Power Systems*, vol. 36, no. 6, p. 9095, 2012.

[4] Y. Chen, S. Dai, C. Yang et al., “IEC 61850-based modeling of intelligent distributed feeder automation system,” *Electric Power Automation Equipment*, vol. 36, no. 6, pp. 189–222, 2016.

[5] S. M. S. Hussain, M. A. Aftab, and I. Ali, “IEC 61850 modeling of DSTATCOM and XMPP communication for reactive power management in microgrids,” *IEEE Systems Journal*, vol. 12, no. 4, pp. 3215–3225, 2018.

[6] H. Wang, D. Xiong, P. Wang, and Y. Liu, “A lightweight XMPP publish/subscribe scheme for resource-constrained IoT devices,” *IEEE Access*, vol. 5, pp. 16393–16405, 2017.

[7] C. S. Cho, W. Chen, C. Liao et al., “Building on the distributed energy resources IoT based IEC 61850 XMPP for TPC,” in *Proceedings of the 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, IEEE, Taiwan, China, May 2019.

[8] X. Hou, Y. Chen, B. Xu et al., “Application of extensible message and presence protocol in distributed feeder automation,” *Automation of Electric Power Systems*, vol. 43, no. 4, pp. 228–236, 2019.

[9] X. Chen, B. Xu, Y. Chen et al., “Real-time data fast transmission technology for distributed control of distribution network,” *Power System Protection and Control*, vol. 44, no. 17, pp. 151–158, 2016.

[10] Y. Fan, Q. Wang, H. Peng et al., “GOOSE over UDP transmission mechanism for real-time data fast transmission in distribution network,” in *Proceedings of the Green & Sustainable Computing Conference*, Orlando, FL, USA, October 2017.

[11] C. Tang, Z. Yang, B. Song et al., “A method of intelligent distributed feeder automation for active distribution network,” *Automation of Electric Power Systems*, vol. 39, no. 9, pp. 101–106, 2015.

[12] GB/T 35732-2017, *Technical Specifications of Intelligent Remote Terminal Unit of Distribution Automation*, China Electric Power Press, Beijing, China, 2017.

[13] L. He, *Getting Started with IEC 61850 Applications*, China Electric Power Press, Beijing, China, 2012.

[14] Communication networks and ystems for power utility automation: part 7-2 basic information and communication Structure-abstract communication service interface(ACSI): IEC 61850-7-2.2014.

[15] S. M. Farooq, S. M. S. Hussain, T. S. Ustun et al., “Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages,” *IEEE Access*, vol. 7, pp. 32343–32351, 2019.

[16] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, “Time valid one-time signature for time-critical multicast data authentication,” in *Proceedings of the IEEE Infocom*, pp. 1233–1241, Rio de Janeiro, Brazil, April 2009.

[17] Q. Li and G. Cao, “Multicast authentication in the smart grid with one-time signature,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 686–696, 2011.

[18] C. Ji, J. Kim, J. Y. Lee et al., “Review of one-time signatures for multicast authentication in smart grid,” in *Proceedings of the International Conference & Expo on Emerging Technologies for A Smarter World*, Melville, NY, USA, October 2015.

[19] T. Yip, J. Wang, B. Xu, K. Fan, and T. Li, “Fast self-healing control of faults in MV networks using distributed intelligence,” *CIRED-Open Access Proceedings Journal*, vol. 2017, no. 1, pp. 1131–1133, 2017.

[20] R. Kuntschke, M. Winter, C. Glomb et al., “Message-oriented machine-to-machine communication in smart grids,” *Computer Science-Research and Development*, vol. 32, no. 1-2, pp. 131–145, 2017.