Application of 5G Private Network Based on Quantum Communication Technology in Smart Grid

Hui Xiang*, Yuxiang Lv, Julong Chen, Hao Wu, Hui Wu, Yawen Dong, Hao Chen
Anhui Jiyuan software co., ltd, No.1800 Xiyou Road, High-tech Zone, Anhui Province, CHN
* Corresponding author: huixiang202209@163.com

ABSTRACT

The fifth generation mobile communication (5G) has the advantages of high bandwidth, low time delay and low power consumption, and it can play an important role in all aspects of power transmission, substation, power distribution and electricity consumption, effectively making up for the disadvantages of traditional optical fiber communication and profoundly transforming the power communication network. However, the information security problems brought by the application of 5G technology are gradually becoming prominent. Based on this, a quantum key distribution strategy based on the quality of service (QoS) is proposed to improve the confidentiality of 5G electric power private network application scheme. Finally, the feasibility of quantum communication application in power dispatching system is verified. The test results show that the service quality of 5G private network meets the communication requirements of power grid services, the actual transmission delay of the power grid simulation dispatching data is about 1s, and there is no packet loss.

Keywords: Quantum communication, QoS, smart grid, 5G

1. INTRODUCTION

In recent years, the scale of power grid business has been increasing, and the degree of power grid informatization has been increasing, which has brought great convenience to people's lives. However, the traditional power communication network is mainly to meet the basic communication needs, and the deployment cost and communication capacity are difficult to adapt to the digital intelligent transformation of power grid, which restricts the automation and intelligent development level of distribution network [1].

With the continuous development of new generation communication technology, 5G has obvious advantages in key network indicators, network customization, deployment flexibility, etc [2]. Combined with innovative technologies such as network slicing and edge computing, it can meet the network communication needs of the power industry with ultra-low latency, ultra-high bandwidth and ultra-large scale connection, and provide strong communication network support for related power applications. The deep integration of 5G network and power industry has gradually become an important direction to empower the future ubiquitous power Internet of Things. The low delay characteristic of 5G network can provide real-time communication guarantee for the switch on the pole, and realize the accurate dispatching of power distribution network [3]. In terms of phasor measurement unit (PMU) service of distribution network, the high-precision timing of 5G network perfectly meets the communication requirements of PMU service for timing accuracy and time delay, and provides accurate time scale information for phasor data such as voltage phase and current phase of power system hub [4]. In terms of data collection of distribution network, the connection scale of 5G network per square kilometer is up to one million, which provides an effective communication means for massive data collection of distribution network terminals.

Compared with optical fiber communication and traditional wireless private network communication in power system, 5G has obvious advantages. At the same time, it also brings greater challenges of information security[5]. On the one hand, a large number of 5G edge nodes increase information data exposure and security risk points; On the other hand, there are many users in the 5G network, which puts too much pressure on the existing authentication system and may cause data leakage.

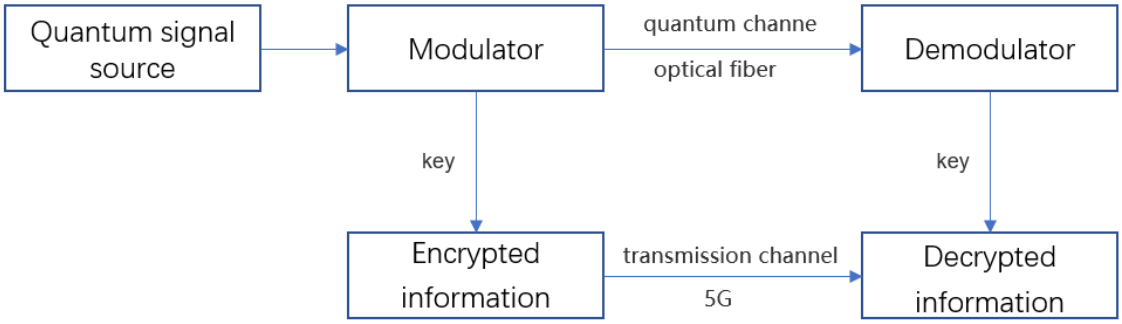
Therefore, how to improve the security performance of 5G power private network is a challenge. At present, the research on electric power secret communication uses various cryptographic algorithms to realize communication encryption, although it can also play a certain role in secrecy, but in the face of increasing hacker attacks, the limitations of

Third International Symposium on Computer Engineering and Intelligent Communications (ISCEIC 2022),
edited by Xianye Ben, Proc. of SPIE Vol. 12462, 1246208 · © The Authors. Published under a
Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.2660932

traditional methods are gradually revealed. Quantum communication technology breaks the limitation of the existing communication mode, completely changes the existing key distribution technology, and ensures that the obtained information technology is difficult to be cracked and eavesdropped, thus realizing completely confidential communication of electric power [6]. Therefore, this paper makes an in-depth study on the application of quantum communication and 5G private network in power grid, and proposes an application scheme of 5G private network based on quantum secure communication to help optimize quantum key distribution strategy based on QoS.

2. ARCHITECTURE DESIGN

This paper mainly studies the application of quantum secure communication based on quantum key distribution (QKD), and mainly adopts BB84 protocol [7]. In this protocol, two groups of conjugate bases and four quantum states are used as the carriers of quantum information. The communication parties first use quantum channels to transmit quantum states, and the sender sends the quantum states encoded by the measurement vectors to the receiver, and the receiver randomly selects the measurement vectors to measure and save the measurement results. Then, the two communication parties use the classical channel to negotiate the key to obtain the original key; Finally, the receiving end announces the partial value of the original key, and both parties make system disturbance or eavesdropping judgment to obtain the final security key, so as to ensure that the whole key distribution process is completed under the condition that the transmission is not eavesdropped [8-9]. The working principle of quantum key distribution is shown in Figure 1. The proposal of BB84 protocol marks the beginning of a new chapter in quantum communication security technology, and BB84 protocol has gradually become a quantum communication protocol with high practical level because of its advantages of good operability and strong stability.



Figures 1. The working principle of quantum key distribution

The 5G-based quantum secure communication and hard-slice private network need to carry important services such as power production, dispatching, inspection and management, and are the key links to build a first-class energy Internet enterprise and improve the elements of power grid security management. The combination of quantum secure communication technology and 5G technology needs multi-dimensional consideration, especially in the face of complex power distribution network services, and it needs to be designed in many aspects according to its characteristics.

When designing the overall system architecture, it is necessary to consider the capability positioning of quantum security technology and 5G slicing technology, and analyze the factors such as equipment type, data volume, time delay requirements and security requirements of distribution network application and distribution master station, so as to design the business of production control area and management information area accordingly. As a data encryption means, quantum security technology takes advantage of the safest communication encryption system at present, and 5G hard-slice network takes advantage of solving the communication pain point of the "last mile" of distribution network as a data transmission means. By deploying quantum security devices and 5G hard-slice private network devices in local companies and distribution network application terminals, quantum security reinforcement of end-to-end data transmission is realized, and data security problems caused by the increasing access of edge nodes to heterogeneous terminals, the increasing number of users and increasingly rich business applications are solved.

3. QUANTUM KEY DISTRIBUTION STRATEGY

3.1 Electric power business classification

There are many kinds of electric power services transmitted by the communication network, such as the electric energy collection service of intelligent meter reading system, the relay protection service of monitoring electric power equipment, etc. There are three common types of power business classification: 1) according to the real-time requirements of power business, it can be divided into real-time power business and non-real-time power business; 2) According to the safety management system of power grid, the electric power business can be divided into four safety zones I, II, II and IV, among which the electric power business in the first and second safety zones is related to the production control of power grid, and the electric power business in the second and fourth safety zones mainly assists the production control of power grid and realizes the informationization of enterprise management; 3) According to DL/T 5391-2007 standard, electric power services can be divided into data services, voice services, video services and multimedia services[10]. This paper only considers some electric power services, including relay protection, wide-area vector measurement, dispatching telephone, dispatching automation, electric energy metering and telemetry, substation video monitoring, video conference, protection information management, administrative telephone, lightning location detection and office automation. The characteristics and communication indexes of each electric power service are different [11].

There are different QoS requirements for the services in the electric power network. According to the characteristics of electric power services and the requirements of communication indicators, this paper divides the electric power services into three categories, including Expedited Forwarding (EF), Assured Forwarding (AF) and Best-effort (BE) [12], as shown in Table 1.

Table 1. Electric power business classification

Type of service	Electric power business
Expedited Forwarding, EF	relay protection
Assured Forwarding, AF	wide-area vector measurement, dispatching telephone, dispatching automation, electric energy metering and telemetry, substation video monitoring, video conference, protection information management, administrative telephone, lightning location detection. etc.
Best-effort, BE	office automation.

3.2 Distribution strategy

At present, the hardware performance of quantum communication equipment is firstly, especially the quantum key generation rate of QKD equipment is limited. At the same time, due to the application of 5G network and the huge demand of power grid service scheduling, the way of generating a key once per service scheduling is unsustainable. Through in-depth investigation of power dispatching business, it is decided to adopt different key distribution strategies to deal with this problem. According to the relative importance of scheduling services, the application forms of quantum keys are divided into three forms: one secret at a time, high-order session keys and low-order session keys, and their security levels decrease in turn. The details are as follows.

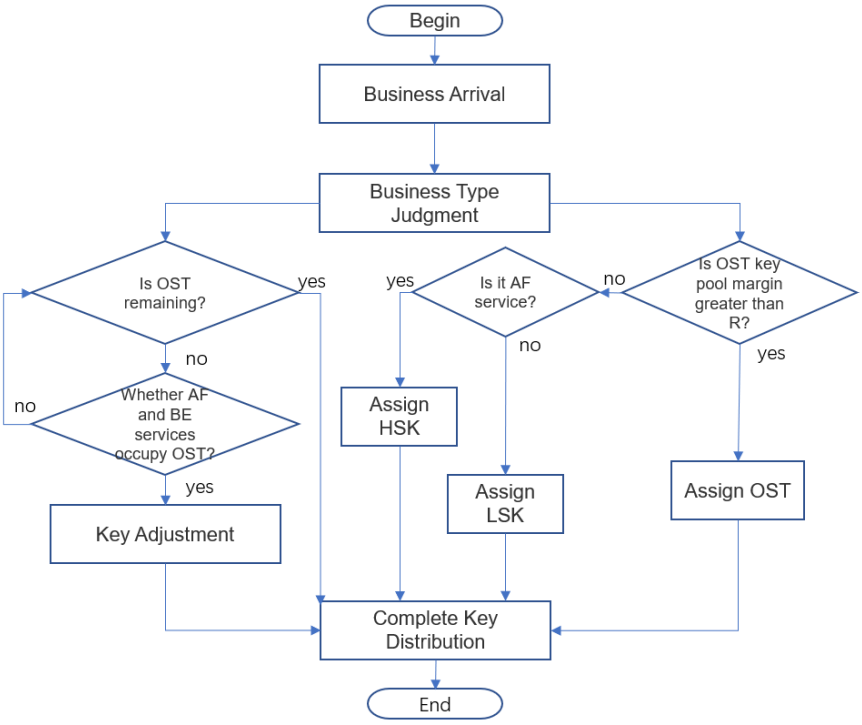
(1) One secret at a time (OST): the quantum key consumed is as long as the encrypted data.

(2) High-level session key (HSK): AES-256 encryption algorithm is set, and the length of data packet and key used for each encryption is 256 bit.

(3) Low-level session key (LSK): AES-128 encryption algorithm is set, and the length of data packet and key used for each encryption is 128 bit.

The power dispatching system based on 5G technology has the characteristics of multi-site and high traffic flow, and the variability of the system state easily affects the use of quantum keys, such as the renewal and expansion of the business system and the handling of special emergency situations, which will all lead to the shortage of quantum keys. Therefore, a quantum key allocation strategy based on QoS is proposed according to the business types of the sites, and the specific process is shown in the figure 2. The specific core idea is: according to the QoS requirements of each service, judge the

service type, divide the importance of EF, AF and BF services into three priorities: high, medium and low, and choose the encryption key form according to the service importance. For the EF electric power business, it has the highest requirement for security, so it is preferred to assign one-time encryption. If there is no surplus in the one-time encryption key pool, it is necessary to adjust the existing AF and BF businesses that assign one-time encryption keys, so as to ensure the use of AF business first. When that arrive service is a non-AF service, firstly, it is judged whet the remaining amount of the one-time secret key pool is greater than R, if it is greater than R, a one-time secret key is assign to it, and if the remaining amount is less than R, a high-order session key is assigned to AF service and a low-order session key is assigned to BE service.



Figures 2. Quantum key allocation strategy based on QoS

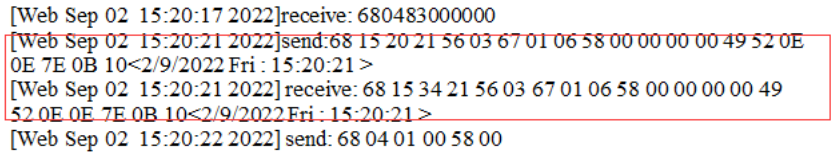
4. TEST ANALYSIS

In order to verify the effectiveness of the key distribution strategy based on quantum communication designed in this paper, the above-mentioned quantum key distribution system in power grid environment is analyzed. The quantum key distribution equipment selected in this paper is phase coding equipment based on FM system, including a set of QKD transceiver equipment and a set of virtual private network (VPN) equipment. The equipment used for the validation of the experiment is shown in the table:

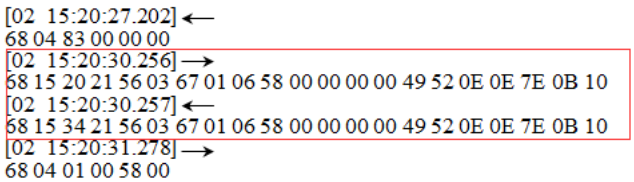
Table 2. Experimental installation

Device Name	Equipment Type
QKD 1	QKD-PHA1250A-S
QKD 2	QKD-PHA1250A-S
Key management service	NF-5270 M3
System Video telephone server	eSpace U1910
quantum VPN device	500Mbps, and supported encryption algorithms include DES, 3DES, AES, SM1, SM4, etc.

In the above experimental system, VPN establishes a secure tunnel, loads the power grid simulation dispatching data, and encrypts and transmits the power grid simulation dispatching data in real time; Collect message data, as shown in Figures 3 and 4, which are the main station message and the sub-station message.



Figures 3 main station message



Figures 4. sub-station message

The box area in Figure 3 and 4 indicates the sending and receiving time of real-time messages. The time for observing messages in two stations is 30s and 21s, respectively, and the transmission delay difference is about 9s. Because the difference between the time of the main station system and the time delay of the sub-station system is about 8s, the actual transmission delay of the power grid simulation dispatching data is about 1s, and there is no packet loss, which meets the standard requirements. The feasibility of power dispatching system business transmission in quantum communication system is verified.

5. CONCLUSION

The application of quantum communication technology in the power grid will have certain significance for the security protection of the power grid. In this paper, in the environment of 5G private network and quantum optical cable, a quantum key distribution device suitable for power grid operation is set up, and a quantum key distribution strategy based on QoS is proposed under the condition of stable operation of QKD device, which solves the problem that the low generation rate of quantum keys of QKD equipment leads to some business security exposure, and provides theoretical guidance for the practical application of quantum key distribution technology in power system. Through the transmission of power grid simulation dispatching data service, the actual test parameters meet the transmission requirements, and the feasibility verification of transmission of power dispatching system service in quantum communication system is completed. The next step will be to study the application performance of this algorithm in more complex scheduling data network architecture.

REFERENCES

[1] Zhang J, Wang H , Hu Y , et al. Design of Intelligent Inspection System for Distribution Network Based on Circular Multi-Agent Structure [J]. IOP Conference Series: Earth and Environmental Science, 2019, 218(1):012136 (6pp).

[2] Haider N, Baig M Z, Imran M. Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends[J]. 2020.

[3] Rui W U, Tao J Y. Simulation Research on Speech Compression and Recognition of Mine Wireless Through-the-earth Communication [J]. Computer Simulation, 2018.

[4] Baranda J, Mangues-Bafalluy J, Martinez R, et al. 5G-TRANSFORMER meets Network Service Federation: design, implementation and evaluation[C]. 2020 6th IEEE International Conference on Network Softwarization (NetSoft). IEEE, 2020.

[5] Yang C Y, Ling Y, Li X. Research on Information Encryption Algorithm under the Power Network Communication Security Model[J]. Journal of Physics: Conference Series, 2021, 1852(3):032007 (7pp).

[6] Hu J , Guo L J , Xiao L , et al. The Design and Application in Secure Communication Based on Quantum Technology. 2021.
[7] Xiong P . The Comparison of Secure Key Rate of BB84 Protocol Using Single Photon Detectors and Optical Homodyne Detectors[J]. Journal of Physics: Conference Series, 2021, 1936(1):012021 (7pp).
[8] Korkmaz U , Turkpence D . Transfer of quantum information via a dissipative protocol for data classification[J]. Physics Letters, A, 2022(426-).
[9] Guo J , Du Y , Wu X , et al. An Anti-Quantum Authentication Protocol for Space Information Networks Based on Ring Learning with Errors[J]. Journal of Communications and Information Networks, 2021(6-3).
[10] Radhakrishnan P , Ramaiyan K , Vinayagam A , et al. A Stacking Ensemble Classification Model for Detection and Classification of Power Quality Disturbances in PV Integrated Power Network[J]. Measurement, 2021, 175(2):109025.
[11] Wang W, Wang X, You Z, et al. Research on key node identification method in electric power communication network [J]. Dianli Xitong Baohu yu Kongzhi/Power System Protection and Control, 2018, 46(1):44-49.
[12] Tong L, Gan C, Xie W, et al. Priority-based mode transformation algorithm in a multisystem-based virtual passive optical network[J]. Optical Switching and Networking, 2019, 31(JAN.):162-167.