Innovative Design and Intelligent Manufacturing
L.C. Jain et al. (Eds.)

doi:10.3233/FAIA241095

Research on the Application of Power System Cryptography Based on Quantum Key

Wu DONG[a,1], Xu LIU[a], Linyu PENG[a], Kang LIU[a], Dili PENG[a], Tao WANG[a], Ji SHI[a], Jun ZUO[a]
[a]*Power Dispatching Control Center of Guizhou Power Grid, Guiyang 550002, China*

Abstract. The research and test of the security protection technology of distribution network quantum encryption information based on 5G multi access edge computing applies the communication technology and quantum encryption technology of 5G power private network to the terminal environment of distribution network. Through the integration of quantum key and power service master station, terminal and quantum key, 5G communication and quantum encryption equipment, It enables safe communication between the distribution terminal equipment and the distribution master station, and the system response time is controllable. The results show that in the 5G deployment environment, the maximum delay in 1000 tests is 121.23 ms, while in the 5G+quantum environment, the maximum delay is 200.23 ms.

Keywords. Distribution network; quantum encryption; multi-access edge computing; information security

1. Introduction

Power system is an important cornerstone of national development. A stable power system provides a strong energy guarantee for industrial production, people's life and urban and rural social management, which puts strict requirements on the information security of the power system [1]. With the rapid development of power grid informatization, the related work has reached the advanced level in the world, and it has the ability of real-time information collection, multi-regional and multi-level collaborative scheduling, various data analysis and accident handling [2]. The rapid development of data acquisition and processing technology has built a solid foundation for power grid informatization, which has enabled the power system to accumulate a large number of high-value data, such as power generation capacity, enterprise energy consumption data, customer contact information, detailed address and other information, which must be secured.

Quantum secure communication is a new means of information security communication, which is different from the traditional mainstream encryption methods such as RSA, which uses factorization of large numbers (that is, a large integer is decomposed into the product of several prime numbers, which is far from easy to

[1] Corresponding Author: Wu DONG GZDWdongwu@163.com

multiply several prime numbers) or discrete logarithms and other mathematical problems. It is based on the basic principles of quantum physics as security [3]. The intractability of mathematical problems is relative to that of classical computers, and will be threatened by the improvement of computing power and the birth of quantum computers. However, the basic principles of quantum physics have no such risk. Therefore, quantum secure communication is the only secure communication method that has been theoretically proved to be "unconditionally secure" so far [4]. Quantum secure communication has also attracted the attention of many engineers in the power industry, and its application in the power industry has achieved good results.

2. Literature Review

The secret transmission of information can not be separated from encryption. At present, the mainstream encryption scheme is asymmetric encryption scheme represented by RSA algorithm. The security of such encryption schemes depends on the difficulty of classical computers in solving specific problems (such as factorization problems). The BB 84 protocol is the first one proposed to take the physical characteristics of quantum mechanics as the guarantee, which can detect eavesdropping and solve the insecure factors of classical secure communication, and can ensure the security of information transmission to a certain extent [5]. So far, BB84 protocol is still the most influential quantum key communication protocol. Amer, O. et al. proposed a quantum secure communication protocol based on continuous variables [6]. Tang, Z. et al. proposed a continuous variable QKD protocol - GG02 protocol [7], which loads information on the x and p components of the coherent state. Portmann, C., et al. proposed the double decoy state QKD protocol and the infinite dimensional decoy state QKD protocol for PNS attacks, and carried out strict experimental tests. The test results gave a strict security proof [8]. Shim, K. A. and others strictly proved the security of CVQKD against a finite length key under coherent attack by using the rotation invariance in space [9]. Tang, Z. et al. proved that the coherent state CVQKD protocol is combinatorial security under coherent attack, and can also fully prove the theoretical security of the Gaussian modulated coherent state CVQKD protocol [10].

In order to enhance the potential of power system control and make full use of massive communication resources, information reinforcement and protection must be carried out. The integration of 5G power virtual private network+quantum encryption information security protection technology in the field of distribution network, and the establishment of wireless security access information security protection technology system for distribution network business can not only ensure more secure and reliable operation of power system, but also effectively reduce the cost of construction, operation and maintenance.

3. Research Methods

3.1. Distribution Network Terminal Situation

The distribution network terminal mainly refers to the terminal equipment in the intelligent distribution network system, which is used to monitor, control and manage the power grid. It is one of the important components of the smart grid, and it mainly

manages and processes all kinds of data in the distribution network through information and communication technology. Distribution automation is a process of intelligent management and control of distribution system by using advanced information, communication and control technology. Through the distribution automation system, real-time monitoring, remote operation, automatic adjustment and fault diagnosis of the distribution network can be realized, so as to improve the operation efficiency, reliability and safety of the power grid [11].

At present, the common distribution network automation terminals mainly include distribution terminal unit (DTU), feeder terminal unit (FTU) and substation area intelligent convergence terminal unit (TTU). DTU is mainly installed in conventional switching stations/stations, outdoor small switching stations, ring network cabinets, various substations, etc., to complete the acquisition and calculation of the position signal, voltage, current, active power, reactive power, power factor, electric energy and other data of the switchgear, and to conduct opening and closing operations to achieve fault identification Isolate and restore power supply to non-fault section; FTU is a switch monitoring device installed beside the feeder switch, which is responsible for monitoring the on-off of the load switch on the overhead line; TTU mainly monitors and records the operating status of distribution transformers, calculates the effective value of primary voltage, effective value of current, active power, reactive power, power factor, active energy, reactive energy and other operating technical parameters regularly according to the three-phase voltage and current sampling values at the low-voltage side, and records and stores them for a period of time.

3.2. Power 5G Virtual Private Network

The power 5G virtual private network refers to a virtual private network for the power industry through wireless transmission, bearer network, core network, forwarding data and other links based on network slicing, multi access computing (MEC) and other technologies in the operator's 5G network, which can realize cross domain integration with the power information communication private network, and complete the end-to-end business carrying High reliable security isolation and communication resource management. 5G MEC is a mobile edge computing technology, which makes data processing and storage more closely connected to users, thus improving the speed and efficiency of mobile networks. In the field of electric power, 5G MEC enables faster data transmission and lower latency, thus supporting the realization of smart grid.

At the same time, the power 5G virtual private network needs to meet the basic security protection requirements of the power industry, that is, the principle of "security zoning, network dedicated, horizontal isolation, vertical authentication". In particular, for power production control business, the 5G virtual private network of power needs to be dedicated to the network equivalent to physical isolation, so the relevant private network elements in the production control region should be deployed independently to meet the security protection requirements of the power monitoring system (GNA [2015] No. 36).

3.3. Quantum Encryption Information Security Protection Technology

With the combination of quantum mechanics and information science, quantum information technology has gradually formed, in which quantum encryption technology is used more frequently. Quantum encryption technology is a quantum random number

generator (QRNG) that generates true random numbers by measuring the intrinsic random characteristics of quantum physical systems. The randomness of keys output each time is formed by the basic principles of quantum mechanics, which is more secure than the generation of other random numbers. Therefore, the quantum encryption security service platform and encryption module are developed by taking advantage of the ever-changing nature of light quanta to produce unpredictable results. Every time the data transmitted is encrypted through this module. Due to the "random generation, one change at a time" characteristic of quantum keys, it can ensure that the interaction instructions are not easy to be cracked.

3.4. Quantum Encryption Information Security Protection Scheme Design

3.4.1. Quantum Encryption and Distribution Network Rehabilitation Works

In recent years, China has made breakthroughs in the field of quantum information technology. In specific applications, not only based on the wired optical fiber network and quantum key distribution technology, the Mozi satellite is launched to form a satellite ground integrated transmission system, and a quantum key distribution network of a certain scale is formed to provide users with more secure and reliable point-to-point quantum information protection means; In addition, combined with the application of quantum key distribution technology, 4G/5G wireless communication technology can access a large number of wireless terminal devices and business applications to improve the overall security of wireless communication networks.

3.4.2. Composition of MEC Based Quantum Encryption Application Architecture

The existing quantum key distribution network consists of quantum key distribution equipment, optical quantum true random number generator and quantum security gateway. The optical quantum true random number generator can generate a large number of quantum keys, which are uniformly managed by the key management system, and then pushed to the distribution network services and terminals that need to use quantum keys through the quantum security service platform. Based on the quantum key distribution network environment, the application gateway of quantum key is moved forward, and the protection is moved forward to the wireless security access area, and the application mode of quantum security service platform based on 5G network is proposed. The system generates a quantum key through the quantum key distribution network. After registration in the quantum security service platform, the quantum key is filled into the quantum key mobile media (TF card, U-Key, etc.) through the quantum key filling method, and then used for the quantum mobile terminal.

4. Technology Applications

4.1. Design of the Application Environment

Distribution automation applications can achieve highly reliable distribution network protection, rapid fault location and isolation, rapid recovery, accurate load control, efficient transmission of video monitoring, etc. through the use of 5G power virtual private network. In the actual use process, the whole 5G distribution network quantum encryption environment mainly includes the quantum security service platform

(application service side) deployed in MEC, 5G security capability interaction in the transmission process, and the quantum encryption module (terminal side) applied in the distribution terminal.

The quantum security service platform mainly includes quantum key generation, quantum key unified scheduling management and quantum key application at both ends [5–6]. On the application service side, quantum key generation mainly uses the quantum random number generator to generate keys with unpredictable results, and then carries out quantum encryption to form the final encrypted quantum key. In the process of unified scheduling and management of quantum keys, quantum key management machine, exchange cipher machine, quantum cipher service platform and quantum key filling system are also needed. The quantum key management machine is mainly responsible for managing and storing quantum keys; The exchange cipher machine is mainly responsible for controlling the output and exchange of quantum keys in the transmission process; The quantum cryptography service platform is mainly responsible for the external scheduling and use of quantum keys to ensure that the quantum keys can be safely and orderly distributed to the application systems to be used; The quantum key filling system is mainly responsible for filling the quantum key through the U-Shield/TF card and other methods, and using it at the quantum encryption terminal to ensure that the initial key is also secure. On the terminal side, the quantum encryption terminal consists of a quantum security gateway, a quantum encryption module and a 5G transmission terminal (such as the client device CPE). By using the quantum security encryption transmission channel, the security level of 5G terminal access and transmission is improved to ensure that the power business system network transmission is more secure and reliable.

4.2. System Testing

4.2.1. Delay Testing

Select the distribution network DTU for testing, use laptop 1 to simulate 104 master station, and laptop 2 to simulate local master station. The DTU terminal is connected to the local master station system through 5G CPE wireless, and the other end is connected to the test laptop 1 for “three remotes” (telemetry, remote signaling, remote control) test. The message delay time can be obtained by comparing the time difference of the same message received by 104 master station and the local analog master station, as shown in Figure 1. At the same time, 5G environment and 5G+quantum environment are deployed on the master station side for transmission test.

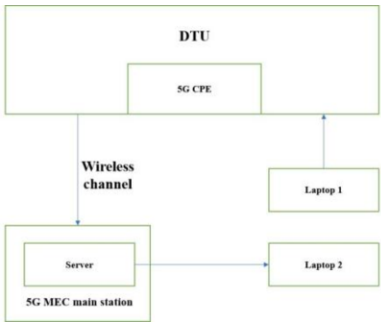

Figure 1. DTU Terminal Test.

The test results show that in the 5G deployment environment, the maximum delay in 1000 tests is 121.23 ms, while in the 5G+quantum environment, the maximum delay is 200.23 ms, which meets the communication requirements of the distribution network.

4.2.2. Delay Test Under Telecommunication Mutation

The DTU terminal connects to the local master station system by using 5G CPE wireless, and analyzes the time scale time difference of SOE between the receiving time of the master station message and the generation time of the message through the remote signaling mutation, that is, the message delay time can be obtained. Relevant data of "three remotes" are obtained through test, as shown in Table 1, 2 and 3.

Table 1. Remote signaling test of 5G DTU.

Telecommuting	SOE occurrence time	The background receives the time of the transposition	Delay time difference/ms
The handles are far away	16:45:14.994	16:45:15.383	489
Put your hands on the ground	16:45:18.833	16:45:19.254	411
Outlet cabinet #1 in place	16:45:49.830	16:45:50.259	429
Outlet cabinet #1, far side	16:45:53.445	16:45:53.896	451
Outlet cabinet No. 1 is in position	16:45:26.423	16:45:26.814	491
Outlet Cabinet Subdivision No. 1	16:45:13.072	16:45:13.483	411
Outlet cabinet #2 in place	16:45:56.498	16:45:56.956	458
Outlet cabinet #2, far side	16:45:59.875	16:46:00.322	447
Outlet cabinet No. 2 is in position	16:46:36.113	16:46:36.519	406
Outlet Cabinet Subdivision No. 2	16:46:38.625	16:46:39.053	428
Battery activation	16:46:44.165	16:46:44.595	430

Table 2. Telemetry test of 5G DTU.

Telecommuting	SOE occurrence time	The background receives the time of the transposition	Delay time difference/ms
Battery voltage	16:45:38.984	16:45:39.418	434

Table 3. Remote control test of 5G DTU.

Remote control of open entries	Backstage prefabrication time	DTU receives the time of prefabrication	Delay time difference/ms
Outlet cabinet No. 1 is in position	16:53:02.508	16:53:03.478	970
Remote control of open entries	remote control execution time	DTU execution time	Delay time difference/ms
Outlet cabinet No. 1 is in position	16:53:03.593	16:53:04.534	941

5. Conclusion

With the construction of a new power system, the continuous access of massive wind power generation, photovoltaic, distributed power and other new energy terminals has intensified the intermittency and volatility of power output. At the same time, the traditional wireless communication mode is difficult to meet the security and reliability requirements of grid related businesses, increasing the potential risk of stable operation of the grid. Aiming at the security problem of wireless communication in distribution network terminals, the introduction of quantum encryption protection technology in the MEC environment of power 5G wireless network is proposed to provide security support for the use of "three remote" functions in distribution automation services. The test proves that the system response time of the application of this scheme meets the requirements of power business specifications. In the future, the "three remotes" and other functions can be continuously released to significantly shorten the time for fault isolation and power transmission recovery, and also provide technical support for rapid fault location and isolation recovery, as well as precise load control, real-time video monitoring, etc.

Funding

This research was funded by Southern Power Grid Corporation Technology Project, grant number 066500KK52222057

References

[1] Ahn, J., Kwon, H. Y., Ahn, B., Park, K., Kim, T., Lee, M. K., ... & Chung, J. (2022). Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd). Energies, 15(3), 714.
[2] Kong, P. Y. (2020). A review of quantum key distribution protocols in the perspective of smart grid communication security. IEEE Systems Journal, 16(1), 41-54.
[3] Alshowkan, M., Evans, P. G., Starke, M., Earl, D., & Peters, N. A. (2022). Authentication of smart grid communications using quantum key distribution. Scientific Reports, 12(1), 12731.
[4] Sharma, M., Choudhary, V., Bhatia, R. S., Malik, S., Raina, A., & Khandelwal, H. (2021). Leveraging the power of quantum computing for breaking RSA encryption. Cyber-Physical Systems, 7(2), 73-92.
[5] Zhou, Y., Tang, Z., Nikmehr, N., Babahajiani, P., Feng, F., Wei, T. C., ... & Zhang, P. (2022). Quantum computing in power systems. IEnergy, 1(2), 170-187.
[6] Amer, O., Garg, V., & Krawec, W. O. (2021). An introduction to practical quantum key distribution. IEEE Aerospace and Electronic Systems Magazine, 36(3), 30-55.
[7] Tang, Z., Zhang, P., & Krawec, W. O. (2021). A quantum leap in microgrids security: The prospects of quantum-secure microgrids. IEEE Electrification Magazine, 9(1), 66-73.
[8] Portmann, C., & Renner, R. (2022). Security in quantum cryptography. Reviews of Modern Physics, 94(2), 025008.
[9] Shim, K. A. (2021). A survey on post-quantum public-key signature schemes for secure vehicular communications. IEEE Transactions on Intelligent Transportation Systems, 23(9), 14025-14042.
[10] Tang, Z., Qin, Y., Jiang, Z., Krawec, W. O., & Zhang, P. (2020). Quantum-secure microgrid. IEEE Transactions on Power Systems, 36(2), 1250-1263.
[11] Zhao, B., Zha, X., Chen, Z., Shi, R., Wang, D., Peng, T., & Yan, L. (2020). Performance analysis of quantum key distribution technology for power business. Applied Sciences, 10(8), 2906.