
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 3, pp. 1818–1825, DOI 10.12694/scpe.v25i3.2723

APPLICATION OF BIG DATA ANALYSIS AND INTELLIGENT ALGORITHM IN POWER SYSTEM OPERATION OPTIMIZATION

HUICHAO JIN, JUNYI HUO, QINGFEN WANG, AND DEXIONG LI*

Abstract. The power communication system provides powerful technical support for realizing the intelligent operation and information management of the power grid and improving the operation efficiency and power supply quality of the power grid. Quantum key distribution (QKD) is considered one of the most promising technologies for commercialization. QKD uses a single photon to encrypt data to produce a more secure and reliable password. This paper intends to study the hierarchical, centralized control architecture of power dispatching based on quantum essential supply (QKD). The performance indexes of MDI-QKD under symmetric and asymmetric conditions were studied by local optimization. The optimal key formation rate of the algorithm is analyzed. From the perspective of quantum critical utilization, a quantum key utilization scheme for grid backbone dispatching service is proposed. The dynamic adjustment test of multi-node time slot and service key update rate is carried out. Experiments show that the MDI scheme can effectively improve the effectiveness of a multi-node QKD system. Thus, the security of data transmission of the core business of power dispatching data networks can be ensured to the greatest extent. AMDI can effectively reduce the transmission timeout of low-priority data streams because the delay of high-priority data streams reaches the proportion. It can be an excellent solution to the power system and the password requirements.

Key words: Power dispatching; Quantum key; Dynamic regulation; Intelligent algorithm; Power Grid System

1. Introduction. With the deepening of quantum cryptography research, its promotion and application have attracted the attention of many enterprises that need high-security performance. Communication is a significant auxiliary means in the operation of the power grid. The power communication system provides powerful technical support for realizing the power grid's intelligent operation and information management, improving the operation efficiency and power supply quality. With the expansion of the scale and scale of the power grid, the power communication system as the monitoring and operation information of the power grid has become more and more complex. The safety of power communication is directly related to the safety of the whole power grid. The need for secure and reliable transmission of network information is more urgent, especially for the power network with UHV network as the core and coordinated development of power grids at all levels.

This paper presents a new power communication technology based on quantum cryptography. The use of quantum cryptography technology to achieve high-capacity and high-rate secure transmission is a research hotspot. Therefore, how to effectively use quantum communication technology is currently a hot topic worldwide. Quantum key distribution (QKD) is considered one of the most promising technologies for commercialization. QKD uses a single photon to encrypt data to produce a more secure and reliable password. There are some essential principles in quantum physics, such as the principle that single photons cannot be divided, the Heisenberg uncertainty relation, the principle of measuring collapse, and the principle of non-cloning. This makes quantum cryptography completely secure in theory. Therefore, the algorithm has a high coding rate. Using quantum communication technology to transmit secret information in practical applications is very difficult. It is difficult to achieve the goal of complete secrecy of grid services. It is necessary to select some essential data streams and use quantum cryptography to encrypt them to ensure data security. In this paper [1], Fuzzy logic is used to adjust the weight of the SMDI algorithm dynamically. This method can adjust the weights according to the delay and throughput rate to improve equity and service quality.

Reference [2] proposes an improved SMDI method. The algorithm adjusts each queue's weight by the buffer size so that the delay between each queue can be balanced. Reference [3] adds a strict priority queue

*Department of Electrical Engineering, Shijiazhuang Institute of Railway Technology, Shijiazhuang, Hebei, 050041, China (Corresponding author, LiDexiong200@163.com)

and the Low Delay queue (LLQ) algorithm. This method can prioritize two types of high-priority services, thus improving service quality. This further increases the likelihood of "hunger" in the low-priority cohort. The existing methods cannot control the network delay directly, so it is difficult to effectively guarantee the service quality of each queue in the network. However, the combined hybrid optimization strategy cannot completely solve the "hunger" problem while ensuring the quality of high-priority queuing service.

2. Modelling and performance optimization of communication system based on MDI. QKD is one of the most practical and promising security technologies. This will provide critical performance optimization for MDI protocols currently in the limelight. The difference with the regular QKD protocol is that there are two sending ends in MDI: Alice and Bob. They send a signal that Charles can detect [4]. If Charles is between Alice and Bob, call it symmetric MDI (SMDI). If Charles is offset at the midpoint, call it an asymmetric MDI (AMDI). Most of them are AMDI in real life. Through the research of this project, it will get the key generation rate of MDI protocol in the case of finite and infinite samples. An infinite set of solutions is an ideal finite solution. In addition, from the existing results, the number of decoy states selected in this paper is 2.

The security key rate obtained by quantum state preparation, transmission, Bell state determination, quantum state screening, parameter estimation, error correction, and privacy amplification in MDI is as follows:

$$S \geq g_d[D_{11}^{C,E}(1 - F_2(e_{11}^{X,V})) - \hat{D}_{\eta_\alpha\eta_\beta}^{C} g_e F_2(\hat{K}_{\eta_\alpha\eta_\beta}^{C})] \tag{2.1}$$

Where g_d is the convention coefficient. The protocol coefficient is $g_d = 1$ for infinite sets. C is a finite set. Here $U_{\eta_\alpha}, U_{C|\eta_\alpha}$ and $U_{\eta_\beta}, U_{C|\eta_\beta}$ are the probability that Alice and Bob transmit the signal state, and the probability that $g_d = U_{\eta_\alpha} U_{C|\eta_\alpha} U_{\eta_\beta} U_{C|\eta_\beta}$ password is selected in this state. Where g_e represents the error correction factor [5]. Where F_e is the binary Shannon entropy. $\hat{D}_{\eta_\alpha\eta_\beta}^{C}$ represents the total amount of detection obtained when both Alice and Bob choose the emission state based on C. Where $\hat{K}_{\eta_\alpha\eta_\beta}^{C}$ is the corresponding bit error. When Alice and Bob both choose the C group to emit a single photon state, $D_{11}^{C,E}$ is the lower bound of the probe. Where $e_{11}^{X,V}$ is the upper bound for detecting the bit error rate under the corresponding X base. $\hat{D}_{\eta_\alpha\eta_\beta}^{C}$ and $\hat{K}_{\eta_\alpha\eta_\beta}^{C}$ are determined by test. In this paper, the superscale ĉan be replaced by the theoretical value provided in the linear channel model of MDI system. The absence of îndicates a corrected data error. These two values are the same regardless of statistical fluctuations [6]. The following analytical formula is obtained by using the Gaussian elimination method:

$$\begin{cases} D_{11}^{C,E} = \eta_\alpha \eta_\beta e^{-(\eta_\alpha+\eta_\beta)} Y_{11}^{C,E} \\ e_{11}^{X,V} = \dfrac{1}{(\lambda_\alpha - \kappa_\alpha)(\lambda_\beta - \kappa_\beta) Y_{11}^{X,E}} (\hat{K}_{\lambda_\alpha\lambda_\beta}^{X} \hat{D}_{\lambda_\alpha\lambda_\beta}^{X} e^{\lambda_\alpha+\lambda_\beta} + \\ \hat{K}_{\kappa_\alpha\kappa_\beta}^{X} \hat{D}_{\kappa_\alpha\kappa_\beta}^{X} e^{\kappa_\alpha+\kappa_\beta} - \hat{K}_{\lambda_\alpha\kappa_\beta}^{X} \hat{D}_{\lambda_\alpha\kappa_\beta}^{X} e^{\lambda_\alpha+\kappa_\beta} - \hat{K}_{\kappa_\alpha\lambda_\beta}^{X} \hat{D}_{\kappa_\alpha\lambda_\beta}^{X} e^{\kappa_\alpha+\lambda_\beta}) \end{cases} \tag{2.2}$$

η_α and η_β are the average number of photons in Alice's signal state, C is the average number of particles in Bob's decoy state, and D is the average number of particles in the vacuum state. $\hat{K}_{\lambda_\alpha\lambda_\beta}^{X}, \hat{D}_{\lambda_\alpha\lambda_\beta}^{X}$ is the total bit error when Alice and Bob choose the X base to transmit the deception state. $\hat{K}_{\kappa_\alpha\kappa_\beta}^{X}, \hat{D}_{\kappa_\alpha\kappa_\beta}^{X}$ is the overall bit error for Alice and Bob to choose the X detector.

The optimal solution is obtained by using the above two methods under infinite sets. Then, the key generation rate of the MDI system and its optimal configuration parameters are given for a particular channel length [7]. The optimal parameters contained in SMDI are η, λ and $\kappa = 5e^{-4}$. Because the positions of the two systems are symmetric, the structural parameters are consistent. The best parameter to consider for AMDI is $\eta_\alpha, \eta_\beta, \lambda_\alpha, \lambda_\beta$.

The statistical jitter effect of the measured variable must be taken into account under the finite set condition. φ simple Gaussian variance method is chosen in this paper [8]. Take A as the standard deviation. The limit value $\sigma = 1 - erf(\varphi/\sqrt{2})$ of the safety factor is obtained. Where $erf(\cdot)$ is the error function. The flutter coefficient is determined as $\delta_d = \varphi/\sqrt{\hat{D}_{d_\alpha d_\beta}^{C} N_{d_\alpha d_\beta}^{C}}$, $\delta_{ed} = \varphi/\sqrt{\hat{K}_{d_\alpha d_\beta}^{X} \hat{D}_{d_\alpha d_\beta}^{X} N_{d_\alpha d_\beta}^{X}}$. Then you can get the upper

Table 2.1: Model input characteristics.

Agreement	E	D_E	$K^C_{\eta\eta}$	$D^C_{\eta\eta}$	Y^C_{11}	D^C_{11}	e^X_{11}	R
SMDI	125	0	2.6175×10^{-2}	2.72×10^{-6}	3.1521×10^{-5}	1.3956×10^{-6}	9.2665×10^{-2}	1.152×10^{-7}
AMDI	115	10	2.3328×10^{-2}	5.1479×10^{-6}	4.9473×10^{-5}	2.4778×10^{-6}	9.001×10^{-2}	1.9118×10^{-7}
AMDI	105	20	2.1775×10^{-2}	8.8574×10^{-6}	7.927×10^{-5}	4.2183×10^{-6}	8.8992×10^{-2}	3.7094×10^{-7}
AMDI	95	30	2.0727×10^{-2}	1.55×10^{-5}	1.2843×10^{-4}	7.3297×10^{-6}	9.2938×10^{-2}	6.4358×10^{-7}

and lower bounds of the measurement results needed to calculate the key rate:

$$\begin{cases} \hat{D}^C_{d_\alpha d_\beta}(1-\delta_d) = \underset{-}{D^C_{d_\alpha d_\beta}} \le D^C_{d_\alpha d_\beta} \le \bar{D}^C_{d_\alpha d_\beta} = \hat{D}^C_{d_\alpha d_\beta}(1+\delta_d) \\ \hat{K}^X_{d_\alpha d_\beta}\hat{D}^X_{d_\alpha d_\beta}(1-\delta_{ed}) = \underset{-}{K^X_{d_\alpha d_\beta}}\underset{-}{D^X_{d_\alpha d_\beta}} \le K^X_{d_\alpha d_\beta}D^X_{d_\alpha d_\beta} \le \\ \bar{K}^X_{d_\alpha d_\beta}\bar{D}^X_{d_\alpha d_\beta} = \hat{K}^X_{d_\alpha d_\beta}\hat{D}^X_{d_\alpha d_\beta}(1+\delta_{ed}) \end{cases} \tag{2.3}$$

The superscript represents the upper bound of the corresponding parameter, and the subscript represents the lower bound of the corresponding parameter. d forη, λ, κ. Replace the upper and lower bounds of (3) with the optimal solution of (2) and (1). The key generation speed of the MDI protocol with a particular channel length is given. The upper and lower bounds are chosen based on the worst-case performance evaluation principle. This is true even when $D^{C,E}_{11}$ becomes smaller and $e^{X,V}_{11}$ becomes larger in the equation (2). At this time, even if $(\kappa, U_{C,\kappa})$ is at rest, SMDI has $\eta, \lambda, U_\eta, U_\lambda, U_{C|\eta}, U_{C|\lambda}$ optimal parameters. However, even if $(\kappa, U_{C,\kappa})$ is constant in AMDI, there are still $\eta_\alpha, \eta_\beta, \lambda_\alpha, \lambda_\beta, U_\eta, U_\lambda, U_{C|\eta}, U_{C|\lambda}$ optimal parameters when the probability coefficients of the two variables are the same.

The optimal analysis of MDI system performance is carried out with $\lambda = 1550nm$ as the light source. The loss of the fiber is $\alpha = 0.2dB/km$. The probability that a photon is projected by the wrong detector is $e_d = 1.5\%$. The dark count of the detector is $Y_0 = 6.02 \times 10^{-6}$. The quantum utilization rate of the device is $\eta_d = 0.145$. The bidirectional error correction factor is $g_e = 1.16$. The safety factor is $\sigma = 5.73 \times 10^{-7}$. Its standard deviation is $\varphi = 5$. The limited data set is $N = 10^{14}$. The light source has a pulse frequency of $g = 10^9 Hz$. Here, the values of N and $g$are large compared to the traditional DS protocol [9]. This is mainly because there are two receivers in the MDI system, and the detection of the Bell state requires the quantum state transmitted by the receiver to conform to a particular entangled state, leading to the MDI system's low-key generation rate. This problem can be effectively solved by increasing N and g. The LSA method is used to optimize its configuration and indexes in detail. The optimized results are compared with those in the literature.

Figure 2.1 shows the best key bit rates for various MDI protocols with different channel lengths. The universal rate value is obtained by multiplying the optimal key rate calculated by formula (1) with the light source pulse frequency g. Table 2.1 and 2.2, respectively, list the optimal features and configurations of each MDI protocol in the specified channel. The optimal index is the detection rate of signal and photon state alone and the bit error rate of detection. The optimal configuration parameters are the signal-to-noise ratio, the number of deception photons and their corresponding configuration parameters. E represents the entire length. D_E represents the distance difference between each end and the detector.

It can be seen from Fig. 2.1 that the calculated security critical distance of SMDI and the three AMDI is 159,157,155,149 km under a finite set of selected security boundary parameters. The maximum at infinite sets is 201 kilometers. When the distance difference between the two transmitting terminals is not very large, AMDI parameters are comprehensively optimized [10]. The critical transfer rate over a distance of 100 km can be obtained, and the result is comparable to SMDI. In addition, this paper also compares the best critical generation speeds obtained by similar algorithms under different device parameters. Compared with DS, the optimal critical generation speed of MDI is about 1/10 of DS. But its crucial generation distance is relatively long.

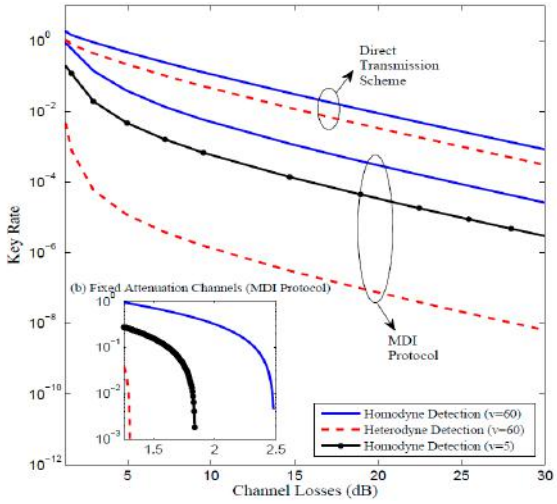

Fig. 2.1: Optimized key bit rate of the MDI protocol.

Table 2.2: Model input characteristics.

Agreement	E	D_E	η_α	λ_α	η_β	λ_β	U_η	U_λ	$U_{C\|\eta}$	$U_{C\|\lambda}$	$U_{C\|\kappa}$
SMDI	125	0	0.289	0.075	0.701	0.235	1.031	0.373	0.253		
AMDI	115	10	0.371	0.083	0.271	0.068	0.642	0.295	1.031	0.414	0.284
AMDI	105	20	0.384	0.084	0.286	0.054	0.655	0.274	1.031	0.420	0.297
AMDI	95	30	0.403	0.063	0.302	0.043	0.657	0.265	1.031	0.425	0.304

3. Research on the application scheme of quantum key based on MDI. Figure 3.1 shows a design unit pattern for abstracting PDDN based on hierarchical centralized control architecture (Picture quoted from Review of Modelling and Simulation Methods for Cyber-Physical Power System). It is cascaded vertically and extended horizontally to form a complex power-dispatching network with multiple structures utilizing reliable Repeaters. The primary station in this table governs two secondary stations and an attached power plant and substation [11]. The solid lines between all the stations are divided into two: one is a quantum line, and the other is a classical line. It is used to transmit and test quantum states in MDI protocol. The dotted line between stations is a typical channel, which realizes typical post-processing and meets the requirements of the protocol. The spacing of stations in this table is determined according to the actual wiring situation of a network province. This paper mainly discusses using the MDI quantum key with a higher security level. If this type of quantum bond is insufficient, it is automatically converted to a lower-level DS or classical bond.

If A type n_s service exists between a pair of QKD nodes, then the number of remaining keys D_t in the corresponding key pool in time window ϕ refers to the difference between the number of keys U_t generated and the number of keys A_t used during this period:

$$D_t = U_t(i) - A_t(i) = R'_t(i)\phi - \sum_{j=1}^{n_s} \frac{N_t(j)}{g_t(j)} V_t(j) \tag{3.1}$$

$N_t(j)$ represents the number of packets to be encrypted in ϕ. $V_t(j)$ represents the number of quantum keys to be used. $g_t(j)$ indicates the update frequency of the service quantum key. Where $R'_t(i)$ is the time-equivalent bit rate of quantum key distribution for the corresponding lines. For n_τ nodes working in TDM mode, the

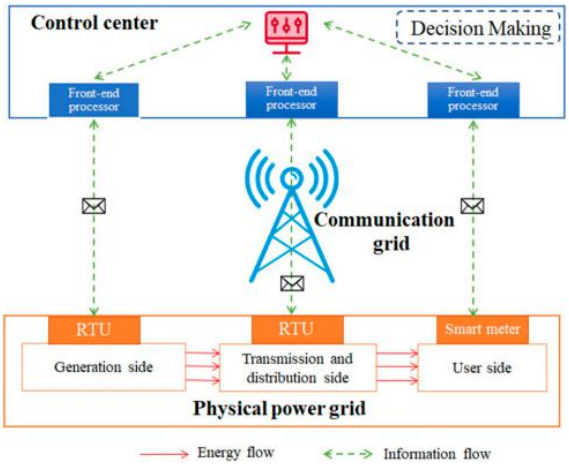

Fig. 3.1: PDDN design unit model.

optimal time interval of each node can be calculated by the following formula:

$$\tau_i = \frac{\frac{A_t(i)}{R_t(i)}}{\sum_{i=1}^{n_\tau} \frac{A_t(i)}{R_t(i)}} \phi \tag{3.2}$$

After using TDM technology, the quantum key distribution rate between each pair of nodes can be equivalent modified as:

$$R_t'(i) = R_t(i) \frac{\tau_i}{\phi} \tag{3.3}$$

Under the condition that the time window after TDM remains unchanged, the key generation and elimination between each node pair obtained by the above method will change [12]. The key generation elimination parameter ζ_{PC} is defined to standardize the characteristics of the key imposed policy. The formula is:

$$\zeta_{PC} = \frac{U_t(i)}{A_t(i)} \tag{3.4}$$

The value of ζ_{PC} should be one or greater. The closer the coefficient is to 1, the more efficient its application in QKD and the better its long-term stability. This design and experimentation will make ζ_{PC} as close to 1 as possible when business data traffic characteristics are determined [13]. The optimal time interval is determined by formula (5). The formula can determine the frequency interval of quantum bond renewal (4) to (6) according to the following process.

4. Simulation analysis. The dynamic adjustment performance is tested in detail by an example. This project aims to test this method's performance under different conditions, especially under abnormal conditions. Based on the Matlab2014a simulation system, four queues are selected for simulation and analysis. Assume that the transmission delay for each queue is $T_1 = 100ms, T_2 = 20ms, T_3 = 300ms, T_4 = 40ms$;. The key length required to encrypt the packet to be encrypted is $L\prime = 128bit$. A quantum critical generation method based on $R = 1\ Mbit/s$ is proposed. Packets queued for encryption obey Poisson distribution, and the arrival rate of packets queued for encryption is the same [14]. The total requirement for the four queue keys is $1Mbit/s$. Because the delay generated by the packet during transmission is much lower than the demand for its transmission delay under normal conditions, this delay can be ignored in the simulation process. Figure 4.1 shows the overall system process, including the application and dynamic adjustment of QKey in practice (Picture quoted from Appl. Sci. 2019, 9(10), 2081).

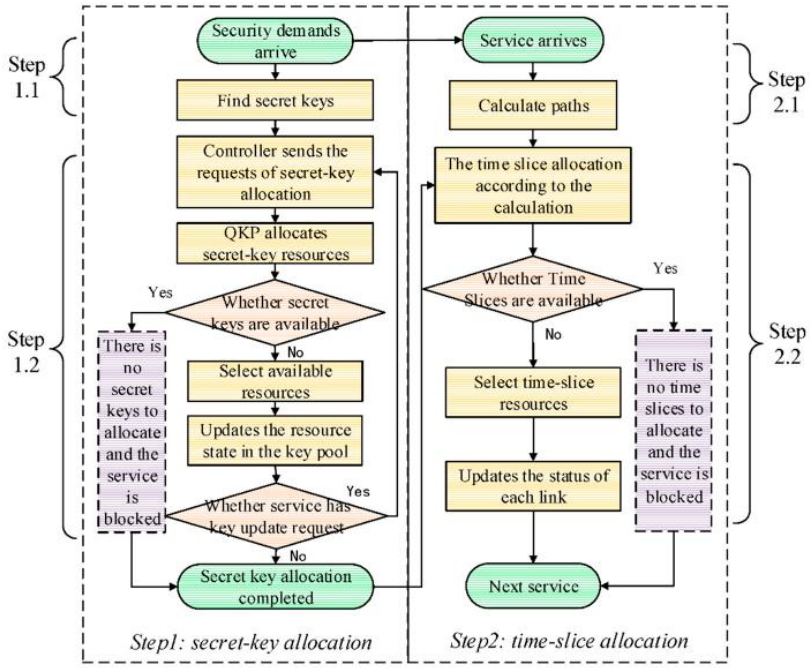

Fig. 4.1: Quantum essential application strategy design and dynamic adjustment process.

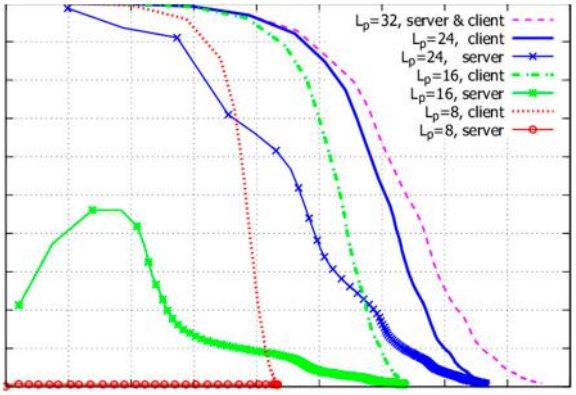

Fig. 4.2: Encryption delay of each queue under SMDI and AMDI algorithms.

The weight $w_1 = 0.3258, w_2 = 0.2504, w_3 = 0.2205, w_4 = 0.2033$ for each set of columns is obtained from formula (1). Each queue received 3000 packets to be encrypted during the simulation. Due to the complexity of the queuing scheduling system and the strong randomness of packet forwarding delay of the data to be encrypted, the average value of 30 simulation results was selected and compared with the SMDI algorithm and the algorithm proposed in reference (Fig. 4.2).

The SMDI algorithm can obtain more scheduling probability when executing tasks because of the higher-weight queue. Moreover, the shorter the time interval for encrypted packets in the queue, the lower the sending delay. Queues with priority four will have a more fantastic exit time for encrypted packets because they have fewer weights. During the queuing process, the network is blocked because of the lack of effective processing [15].

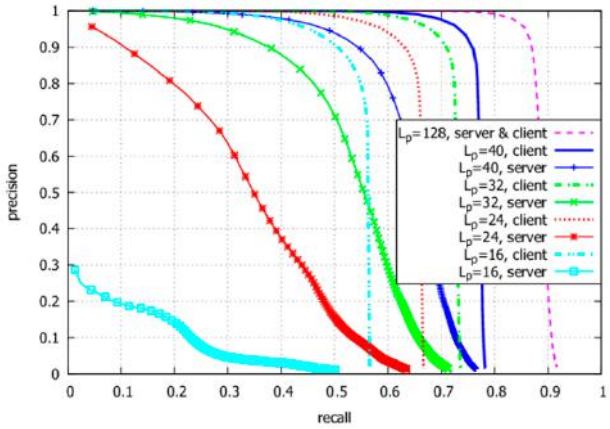

Fig. 4.3: Statistics on the number of timeout data packets.

Finally, the transmission delay of the encrypted information packet exceeds the transmission delay requirement. When the queue length is considerable, the algorithm proposed in reference can appropriately increase the weight of the queue. When queue 4 is congested, it can improve its chances of obtaining a schedule. This algorithm can effectively reduce the queue waiting time but will lead to a slightly longer queue waiting time. Although using this method can make the delay of each queuing system better balanced, it still cannot prevent the phenomenon of a delay exceeding the threshold in the minor queuing system.

The method is simulated by using continuously varying packet arrival rates to explore the optimality of the method to the system performance at different packet arrival rates. The average value of 30 results is calculated to reduce the errors caused by the high randomness of the queuing planning system. In Figure 4.3, the critical requirement rate is the horizontal axis [16]. The aim is to show the effect of the algorithm more directly and reflect the relationship between the critical request rate and the key generation rate. Its value is the number of essential requirements generated at intervals when four queues arrive at a fixed rate.

Because the number of timeout packets in queue 1 is small, it is not listed in item 5. Whereas queue 2 has more time to get more time, the average result of its 30 simulations is still very random. For the rest of the queue, the proportion of timeout packets changes fairly smoothly [17]. Although the algorithm proposed in reference can balance the delay between all queues well, it cannot constrain and optimize the transmission delay with targets effectively. Although the proportion of timeout packets can be reduced by balancing the delay, the optimization results of this method are not significant under the condition of high vital requirements, and its performance is not ideal under the condition of high vital requirements.

The algorithm in this paper can reduce the number of timeout packets. This method can effectively reduce the timeout rate of the system. This method does not significantly affect the timeout rate of high-priority queuing systems while ensuring the transmission delay of queuing systems 3 and 4 to the maximum extent. At the same time, it can effectively reduce the timeout ratio of data packets. Simulation results show that the proposed method has a good delay balance for each queued message waiting for encryption. It can reduce the timeout rate of packets to be encrypted to some extent. The algorithm has good performance for all kinds of crucial requirement rates. In power communication networks, the correctness of the password is more important than the delay. This method can increase the delay under delay tolerance to obtain a higher delay arrival rate. It can solve the cryptographic problem in power communication and improve the efficiency of the quantum key.

5. Conclusion. Due to its limited QKD coding rate, it is only suitable for some essential power services in power communication, so optimizing the quantum cryptographic rate to achieve a reasonable bandwidth allocation is necessary. This paper establishes a quantum communication algorithm based on queueing sort. The method can predict the encrypted packets and schedule the packets that are about to time out preferentially to reduce the timeout of the packets to be encrypted. And it does not significantly reduce the proportion of

packets queued for high priority to be encrypted. When the encoding rate is constant, AMDI can better solve the delay problem of encrypted data. It can implement efficient encryption for more packets to be encrypted. The algorithm can also effectively improve the system's low efficiency of quantum key coding. The simulation results show that AMDI can effectively reduce the transmission timeout of low-priority data streams to ensure the delay ratio of high-priority data streams. It can be a good solution for the power system and password requirements.

REFERENCES

[1] Kuang, R., & Perepechaenko, M. Quantum encryption and decryption in IBMQ systems using quantum permutation pad. J. Commun, 2022; 17(12): 972-978.
[2] Sehgal, S. K., & Gupta, R. SOA Based BB84 Protocol for Enhancing Quantum Key Distribution in Cloud Environment. Wireless Personal Communications, 2023; 130(3): 1759-1793.
[3] Domi Caroline, S. Quantum Key Distribution Algorithm for Network Security. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021; 12(9): 2277-2284.
[4] Cheng, Z., Ye, F., Cao, X., & Chow, M. Y. A homomorphic encryption-based private collaborative distributed energy management system. IEEE Transactions on Smart Grid, 2021; 12(6): 5233-5243.
[5] Yu, X., Liu, Y., Zou, X., Cao, Y., Zhao, Y., Nag, A., & Zhang, J. Secret-Key Provisioning with Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks. Journal of Lightwave Technology, 2022; 40(12): 3530-3545.
[6] Yan, R., Wang, Y., Dai, J., Xu, Y., & Liu, A. Q. Quantum-key-distribution-based microgrid control for cybersecurity enhancement. IEEE Transactions on Industry Applications, 2022; 58(3): 3076-3086.
[7] Al-Balushi, M. A., Alomairi, S. A., & Okedu, K. E. Power situation in Oman and prospects of integrating smart grid technologies. Int. J. on Smart Grid, 2021; 5(1): 45-62.
[8] Liu, Z. Y., Tseng, Y. F., Tso, R., Mambo, M., & Chen, Y. C. Public-key authenticated encryption with keyword search: A generic construction and its quantum-resistant instantiation. The Computer Journal, 2022; 65(10): 2828-2844.
[9] Nematkhah, F., Aminifar, F., Shahidehpour, M., & Mokhtari, S. Evolution in Computing Paradigms for Internet of Things-Enabled Smart Grid Applications: Their Contributions to Power Systems. IEEE Systems, Man, and Cybernetics Magazine, 2022; 8(3): 8-20.
[10] Yan, Y., Liu, Y., Fang, J., Lu, Y., & Jiang, X. Application status and development trends for intelligent perception of distribution network. High Voltage, 2021; 6(6): 938-954.
[11] Mittal, S., & Ramkumar, K. R. Research perspectives on fully homomorphic encryption models for cloud sector. Journal of Computer Security, 2021; 29(2): 135-160.
[12] Wasumwa, S. A. Safeguarding the future: A comprehensive analysis of security measures for smart grids. World Journal of Advanced Research and Reviews, 2023; 19(1): 847-871.
[13] Wang, J., Hong, Y., Wang, J., Xu, J., Tang, Y., Han, Q. L., & Kurths, J. Cooperative and competitive multi-agent systems: From optimization to games. IEEE/CAA Journal of Automatica Sinica, 2022; 9(5): 763-783.
[14] Cai, B. B., Wu, Y., Dong, J., Qin, S. J., Gao, F., & Wen, Q. Y. Quantum Attacks on 1K-AES and PRINCE. The Computer Journal, 2023; 66(5): 1102-1110.
[15] Paramguru, J., & Barik, S. K. Implementation of β-chaotic mapping to improved elephant herding optimisation to dynamic economic dispatch problem. International Journal of Innovative Computing and Applications, 2022; 13(2): 115-125.
[16] Valdez, F., & Melin, P. A review on quantum computing and deep learning algorithms and their applications. Soft Computing, 2023; 27(18): 13217-13236.
[17] Zhang, C., Wu, J., Huang, Y., Jiang, Y., Dai, M. Z., & Wang, M. Constructive schemes to spacecraft attitude control with low communication frequency using sampled-data and encryption approaches. Aircraft Engineering and Aerospace Technology, 2021; 93(2): 267-274.

Edited by: Zhigao Zheng
Special issue on: Graph Powered Big Aerospace Data Processing
Received: Oct 24, 2023
Accepted: Oct 30, 2023