

Protection path and security-metric-based resource allocation algorithm in quantum key distribution optical networks

Li Liu(刘力), Shengtong Zhai(翟晟童), Yao Pu(蒲瑶), and Xu Zhang(张旭)
Citatio: Chin. Phys. B, 2025, 34 (**9**): 090306. DOI: 10.1088/1674-1056/adefd6
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Multicast-oriented key provision in hybrid DV/CV multi-domain quantum networks

Xinyu Chen(陈欣宇), Yuan Cao(曹原), Yuxiang Lu(陆宇翔), Yue Chen(陈越), Kunpeng Zheng(郑昆朋), Xiaosong Yu(郁小松), Yongli Zhao(赵永利), Jie Zhang(张杰), and Qin Wang(王琴)
Chin. Phys. B, 2025, 34 (**9**): 090301. DOI: 10.1088/1674-1056/adecf8

Encoding converters for quantum communication networks

Hua-Xing Xu(许华醒), Shao-Hua Wang(王少华), Ya-Qi Song(宋雅琪), Ping Zhang(张平), and Chang-Lei Wang(王昌雷)
Chin. Phys. B, 2025, 34 (**5**): 050310. DOI: 10.1088/1674-1056/adcdeb

Multi-protocol quantum key distribution decoding chip

Chun-Xue Zhang(张春雪), Jian-Guang Li(李建光), Yue Wang(王玥), Wei Chen(陈巍), Jia-Shun Zhang(张家顺), and Jun-Ming An(安俊明)
Chin. Phys. B, 2025, 34 (**5**): 050303. DOI: 10.1088/1674-1056/adb686

Effect of pseudo-random number on the security of quantum key distribution protocol

Xiao-Liang Yang(杨晓亮), Yu-Qing Li(李毓擎), and Hong-Wei Li(李宏伟)
Chin. Phys. B, 2025, 34 (**2**): 020301. DOI: 10.1088/1674-1056/ad99c9

Multi-protocol relay chaining for large-scale quantum key distribution networks

Yuan Cao(曹原), Xiaosong Yu(郁小松), Yongli Zhao(赵永利), Chunhui Zhang(张春辉), Xingyu Zhou(周星宇), Jie Zhang(张杰), and Qin Wang(王琴)
Chin. Phys. B, 2025, 34 (**1**): 010310. DOI: 10.1088/1674-1056/ad9018

SPECIAL TOPIC — Quantum communication and quantum network

Protection path and security-metric-based resource allocation algorithm in quantum key distribution optical networks

Li Liu(刘力)[1,†], Shengtong Zhai(翟晟童)[1], Yao Pu(蒲瑶)[2], and Xu Zhang(张旭)[1]

[1] *Academy of Communication and Information Engineering , Xi'an University of Posts and Telecommunications, Xi'an* 710121, *China*
[2] *Xi'an Modern Control Technology Research Institute, Xi'an* 710061, *China*

(Received 23 March 2025; revised manuscript received 3 July 2025; accepted manuscript online 15 July 2025)

Quantum key distribution (QKD) optical networks can provide more secure communications. However, with the increase of the QKD path requests and key updates, network blocking problems will become severe. The blocking problems in the network can become more severe because each fiber link has limited resources (such as wavelengths and time slots). In addition, QKD optical networks are also affected by external disturbances such as data interception and eavesdropping, resulting in inefficient network communication. In this paper, we exploit the idea of protection path to enhance the anti-interference ability of QKD optical network. By introducing the concept of security metric, we propose a routing wavelength and time slot allocation algorithm (RWTA) based on protection path, which can lessen the blocking problem of QKD optical network. According to simulation analysis, the security-metric-based RWTA algorithm (SM-RWTA) proposed in this paper can substantially improve the success rate of security key (SK) update and significantly reduce the blocking rate of the network. It can also improve the utilization rate of resources such as wavelengths and time slots. Compared with the non-security-metric-based RWTA algorithm (NSM-RWTA), our algorithm is robust and can enhance the anti-interference ability and security of QKD optical networks.

Keywords: quantum key distribution (QKD), optical network, security metric, protection path

PACS: 03.67.Dd, 03.67.Hk

DOI: 10.1088/1674-1056/adefd6 **CSTR:** 32038.14.CPB.adefd6

1. Introduction

In modern information and communication, security is a key issue that cannot be ignored. Quantum key distribution (QKD) optical networks provide a more secure communication network. Because QKD utilizes the fundamental principles of quantum mechanics to ensure that keys are "information theoretically secure" during transmission. In other words, it does not rely on computational complexity but is based on physical principles, and any attempt at eavesdropping will be discovered. Traditional encryption methods rely on the complexity of mathematical puzzles, but these mathematical puzzles may be defeated with the development of quantum computing. QKD optical networks can effectively protect against this threat and provide a solid defense against quantum computing attacks.[1,2]

In addition, QKD optical networks are extremely flexible in terms of key management and can realize a dynamic, real-time key update mechanism. The new key generated during each communication is used and discarded, making the security of the key independent of the content of the transmitted information, so that even if the key is cracked at some point in the future, the content of the past communication will not be threatened.[3,4] This unique advantage makes QKD optical networks particularly suitable for scenarios that require long-term confidentiality, such as financial transactions, military communications, and transmission of government secrets. QKD optical networks are also highly monitorable, and potential eavesdropping and jamming can be detected in real time during the transmission process, thus providing a double guarantee for security.[5–7] At the same time, QKD distributes keys with the help of quantum channels, eliminating reliance on classical key exchange protocols, thereby reducing vulnerabilities to man-in-the-middle attacks. Therefore, QKD optical networks have gradually become a research hotspot.[8–10]

However, networks are often damaged by external interference, such as data interception and eavesdropping. Path protection mechanisms can effectively solve this issue.[11–14] The protection path algorithm can significantly improve the reliability and security of the network. In addition, the protection path can also increase the anti-interference ability and provide a secure alternate channel to avoid data loss or delay. The design proposed by Gerstel *et al*. enhances network stability while ensuring the continuous and secure transmission of critical data in complex environments.[15] Somani *et al*. consider survivability to be an important consideration for high-capacity networks, as failures can lead to significant degradation of network performance.[16,17] By creating a main and a backup path for every link, optical networks can become more

†Corresponding author. E-mail: liu_li@xupt.edu.cn

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

resilient. Data is often only sent along the main path during regular network operation, switching to the backup path in the event of a failure.[18] Protection paths are also used in QKD optical networks.[19–21] This paper also introduces a protection path mechanism into the QKD optical network to increase the anti-interference ability. When the main path fails, it can be quickly switched to the backup path without disrupting the network.

In QKD optical networks, security is also a key factor to ensure reliable communication.[22–25] With the expansion of network scale and the increase in complexity, how to optimize the resource utilization of key transmission while guaranteeing high security is an important research direction. It is difficult for traditional routing and resource allocation methods to meet the special needs of QKD optical networks.[26] As the number of QKD path requests and key updates increases, serious network blocking problems will occur. Because each optical link has limited resources (such as wavelengths and time slots), this will further exacerbate the blocking problem in the network.[27] So how to reasonably allocate the wavelengths, time slots, and other resources in the QKD optical network has become a key issue. Sharma *et al*. proposed the routing, wavelength, and time slot allocation (RWTA) problem for efficient quantum key pool QKP construction on WDM networks.[28] Wen *et al*. investigated the resulting blocking performance through a series of RWTA algorithms,[29]and they also proposed an LRW weighting mechanism based on the RWTA strategy.[30] Cao *et al*. proposed a new RWTA strategy to allocate three channels (TDCh, QKCh and MBCh) in static scenarios and designed an ILP model and heuristic algorithms for RWTA.[31]

To measure the security of the QKD optical networks, the security level is introduced. It is also important to consider the security levels for different requests due to the different transmission requests in QKD optical networks.[32–34] Sharma *et al*. proposed a priority order-based routing wavelength and time slot allocation (POB-RWTA) algorithm to reduce the blocking of requests for QKD optical paths.[35] Cao *et al*. proposed a secret key-rate sharing algorithm.[36] Ma *et al*. proposed three novel efficient load routing, wavelength, and time slot assignment methods.[37] Ma *et al*. developed two RWTA methods to improve the overall network security performance and the quantum key sharing algorithm by taking into account different security levels.[38] However, none of the above studies considered the effect of path length and the relationship between path length and security level in the QKD optical networks. Therefore, this paper proposes a new algorithm of security-metric-based RWTA (SM-RWTA) by introducing the concept of security metric. The security metric is used to study how path length and security level contribute to increasing security.

In summary, this paper proposes a protection path algorithm with protection mechanism to solve the problem of anti-interference ability in QKD optical networks. The protection path algorithm is to add an additional protection path for each QKD path to protect the main path. This algorithm can significantly improve the success rate of connection requests and reduce the blocking rate of the whole network. Moreover, considering the network security factors, this paper proposes a new RWTA algorithm based on security metric (SM-RWTA). Through simulation analysis, the advantage of SM-RWTA algorithm is that it can prioritize the allocation of resources to higher security metric requests compared with non-security-metric-based RWTA (NSM-RWTA). Furthermore, SM-RWTA can significantly improve the success rate of the key update requests and reduce the network blocking rate. It can also increase the utilization of wavelength and time slot resources and improve the security of QKD optical networks. The rest of the paper is organized as follows: Section 2 introduces the QKD optical network, Section 3 describes the security metric, Section 4 describes the algorithm in detail, Section 5 shows and discusses the simulation results, and Section 6 concludes the paper.

2. QKD optical networks

The QKD network consists of four planes from top to bottom: an application plane, a control plane, a QKD plane, and a data plane. Service requests are generated from the application plane. There are two types of service requests, i.e., the ones with the security requirement and the ones without the security requirement. The serving process of the service request without the security requirement in this architecture is similar to the conventional data transmission. Thus, we only focus on the ones with the security requirement.

Upon receiving service requests, the control plane selects routes and reserves relevant resources for QKChs and MBChs on the QKD plane and for TDChs on the data plane. To facilitate resource allocation for the three types of channels as well as simplify optical network control and management, the control plane is separated from the QKD plane and the data plane and equipped with one or more logically centralized software-defined networking (SDN) controllers, which communicates with the application plane, the QKD plane, and the data plane via control channels.

The working principle of QKD optical networks depends on the unique properties of quantum mechanics, especially the quantum superposition state and the quantum non-clonability theorem. As shown in Fig. 1, the optical network process is that Alice (the sender) and Bob (the receiver) transmit the quantum states (such as quantum bits, qubits) of photons through the quantum channel to generate the encryption key. One of the commonly used protocols in QKD is the BB84 protocol, in which Alice randomly selects a polarized state to send

photons, and Bob randomly selects the measurement basis at the time of reception. With this random data selection, Alice and Bob build an initial key string that contains a certain amount of error codes.

Due to the above characteristics, the QKD optical network architecture is established by combining QKD and optical communication networks. The research in this paper focuses on QKD systems based on optical networks, especially wavelength division multiplexing (WDM).[39–41] WDM can manage quantum and classical channels efficiently. This integration enables scalable key distribution while utilizing existing fiber infrastructure, addressing both resource allocation and security challenges unique to QKD optical networks.[42]

As shown in Fig. 1, in a QKD optical network, three types of channels are required to establish the connection, i.e., quantum key channel (QKCh), measurement basis channel (MBCh) and traditional data channel (TDCh). QKCh is dedicated to distributing secure keys through the transmission of quantum bits (qubits) over optical fiber or free-space links. The quantum states of these qubits are used to generate shared keys between Alice and Bob, leveraging the principles of quantum mechanics to ensure eavesdropping detection. MBCh is responsible for authenticating the key exchange and facilitating post-processing steps. It transmits measurement basis choices, error correction data, and privacy amplification parameters. Although MBCh does not require encryption, it must be secured against active attacks using information-theoretically secure authentication protocols. TDCh is used for encrypted data transmission after key distribution. The shared keys generated via QKCh are applied to encrypt sensitive data which is then transmitted over TDCh to prevent eavesdropping or tampering. These three channels operate synergistically: QKCh ensures the security of key generation, MBCh guarantees the integrity of auxiliary communications, and TDCh enables confidential data transmission.

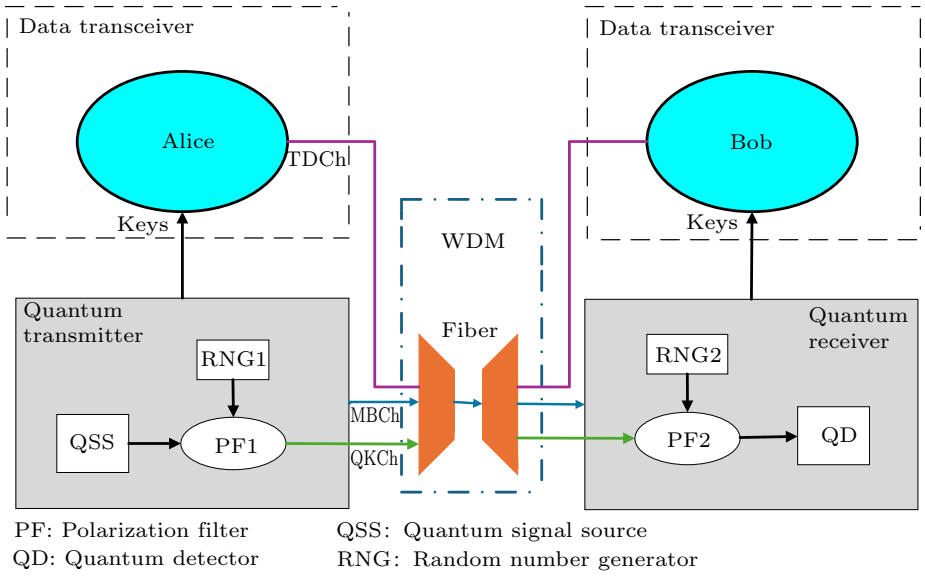


Fig. 1. QKD optical network architecture.

3. Introduction to security metric

We introduce the concept of security metric in QKD optical networks. The security metric is defined as the security level divided by the path length and is used to measure the balance between the security level and the distance when transmitting data. Shorter paths can reduce transmission delays and signal degradation, which do not necessarily have the best level of security. On the contrary, paths with higher security levels often require more complex encryption and authentication mechanisms which result in longer path lengths. By introducing the security metric, QKD optical networks can strike a balance between security and transmission efficiency, ensuring that the selected paths can both effectively resist eavesdropping and attacks and remain highly efficient over a reasonable transmission distance. This metric enables the network to consider security and distance comprehensively when selecting paths, and realize the optimization of key distribution. The following is a description of the security metric.

Security metric (S) is a comprehensive metric used to evaluate the security of a communication path in a QKD optical network. It is defined as the security level of the keys used on the path divided by the length of the path. The specific formula is as follows:

$$S = \frac{K}{L}, \tag{1}$$

where K denotes the security level of the key used to encrypt the data communicated over the path. The key is constantly updated and the key update period T_s measures the frequency of key update. The smaller the key update period T_s is, the more frequent the key update is and the higher the security

level of the key is.[31,47] So the security level K of the key is inversely proportional to the key update period T_s. The security level is usually expressed as an integer and larger values indicate higher security of the key. The security level does not refer to safety. L denotes the number of hops from the source node to the destination node (i.e., the length of the path). The shorter the path length, the less vulnerable it is to attack.

The accumulation of risks hidden by long paths in QKD optical networks is mainly manifested by the fact that the longer the length of the path, the more nodes and links are exposed to eavesdropping and interference which increases the probability of being attacked. This leads to an exponential growth of risk in the system. The reason why the security metric is defined as the security level divided by the length of the path is that it can be normalized to convert the absolute security level into the relative safety efficiency per unit path length.[43,44] It not only avoids the problem of long paths that may hide the accumulation of risks, but also supports users to make rational trade-offs between security and efficiency. So the security metric is both scientific and practical.

The security metric is a comprehensive metric that combines the key security level and the number of hops in a path to provide an assessment of the overall security of a communication path. Compared with a single reliance on the key security level or path length, the security metric can reflect the actual security status of the path more comprehensively. In QKD optical networks, the longer the path length, the more opportunities an attacker may have to eavesdrop or disrupt communications. Therefore, the security metric can more accurately assess the potential risk of long paths by including the factor of path length.

By calculating the security metric, key resources can be allocated more rationally. With limited high-security key resources, priority is given to assigning high-security keys to shorter paths to optimize the security of the overall network. The communication environments and requirements in a QKD optical network may change dynamically. Using the security metric, key distribution policies can be monitored and adjusted in real-time to ensure that communication security is always optimized under different network loads and attack threats. The security metric provides a simple and intuitive numerical value to measure the security of the path. A higher security metric means that the path has higher security under the current key distribution.

In QKD optical networks, the security metric can play an important role in the following aspects:

1. Path selection: When selecting a communication path among multiple available paths, the path with the highest security metric can be prioritized to ensure the security of data transmission.

2. Resource allocation: In the case of limited key resources, the key with a high security level can be reasonably allocated to maximize the security of the overall network by calculating and comparing the security metric.

3. Risk assessment: In the network planning and design stage, potential security risks in the network can be identified and assessed by calculating the security metric of each path.

4. Real-time monitoring: In the planning and design phase of the network, real-time monitoring involves dynamically adjusting key distribution policies during network operation by calculating the security metric of each path.

Therefore, the security metric, as an important index in QKD optical networks, takes into account the key security level and the length of path and provides an effective means to evaluate the security of the communication path. The overall security of QKD optical networks can be significantly improved to ensure the confidentiality and integrity of data transmission by reasonably utilizing the security metric.

Here are the other parameter definitions that will be used in this paper: SKs: secret keys, QLs: quantum links, T_s: key update period, USKs: updated secret keys, LSMRs: low security metric requests, HSMRs: high security metric requests, QCNs: quantum communication nodes, N: number of updates required to update QKD requests.

4. SM-RWTA algorithm based on protection path

In this section, we will first discuss how the protection path works in QKD optical networks and how it acts as a protection to improve the success rate of connection requests. After that, we will discuss how the SM-RWTA algorithm prioritizes requests with high security metric to improve the success rate of key update and reduce the network blocking.

4.1. Protection path algorithm

Protection path is a pre-planned and configured backup transmission channel in network communication, which is designed to quickly take over the communication task when the main path is interrupted due to physical failure, signal interference or security threat to ensure the continuity and reliability of data transmission. In QKD optical networks, the design of the protection path not only needs to meet the requirements of traditional networks in terms of high efficiency and redundancy but also needs to take into account the special characteristics of quantum communication such as the non-clonability of quantum states, the real-time nature of dynamic key update and the security requirements of anti-eavesdropping.

When the main path of a session fails, recovery is usually achieved by recognizing an alternative or backup path. Failure recovery mechanisms are categorized into two types: protection (active) and recovery (passive). In protection mechanisms, resources are identified and preallocated to backup

paths in advance; while in recovery mechanisms, paths are set up only after a failure occurs. The protection mechanism has shorter recovery time and reserved redundant backup capacity. The recovery mechanism is more efficient in terms of resource utilization, but it takes longer to restore the connection and does not guarantee 100% recovery success rate.

Protection and recovery mechanisms are further categorized into link-level and path-level mechanisms. In link-level mechanisms, failures are handled by re-routing traffic. In path-level mechanisms, a link or node-disjoint backup path is computed between the end nodes of each affected optical path. The link-level mechanism is faster and requires fewer control messages, but has higher resource requirements. The path-level mechanism is more efficient in terms of resource utilization, although it has a longer recovery time and higher control overhead.

We assume ideal full-range wavelength converters at every network node, enabling any-input to any-output wavelength conversion. This assumption simplifies resource allocation.[48] By converting signals from one wavelength to another at network nodes to avoid faulty or congested pathways, the wavelength conversion technique improves network resilience and communication continuity when protection paths are switched. It reduces wavelength conflicts and enhances the network's capacity for resource scheduling by enabling data transmission at several wavelengths over the same optical channel. Fast response to protection path switching can be realized by using wavelength conversion technology. During normal network operation, data is usually transmitted only on the primary path, and when the main path fails, the signal can be switched to the alternate wavelength and switched to the protection path for transmission. This method can effectively reduce the impact of network outages and improve the stability and anti-interference ability of communications.

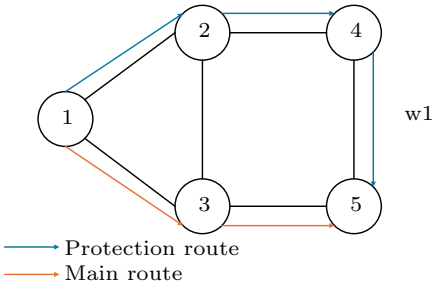


Fig. 2. Schematic diagram of protection path.

Detailed examples of the exact process of the protection path algorithm are illustrated in Figs. 2 and 3. In Fig. 2, at wavelength w1, the calculated shortest path is 1–3–5, so the main path is 1–3–5, and the protection path is set to 1–2–4–5 because the protection path cannot duplicate the main path. In other words, the nodes of the protection pathway cannot be the same as the main pathway. Figure 3 shows that at wavelength w2, when node 3 fails, the target node 5 cannot be reached by using the main path 1–3–5, and then the protection path 1–2–4–5 is used to reach node 5, avoiding network blocking due to the failure of node 3. Thus, the protection path algorithm can improve the success rate of the connection request and reduce the blocking rate.

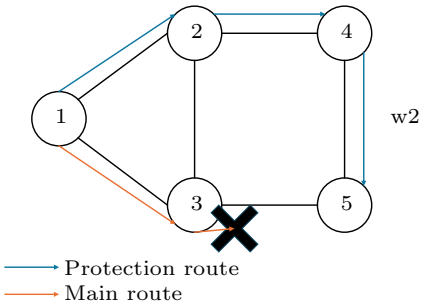


Fig. 3. Schematic diagram of path fault.

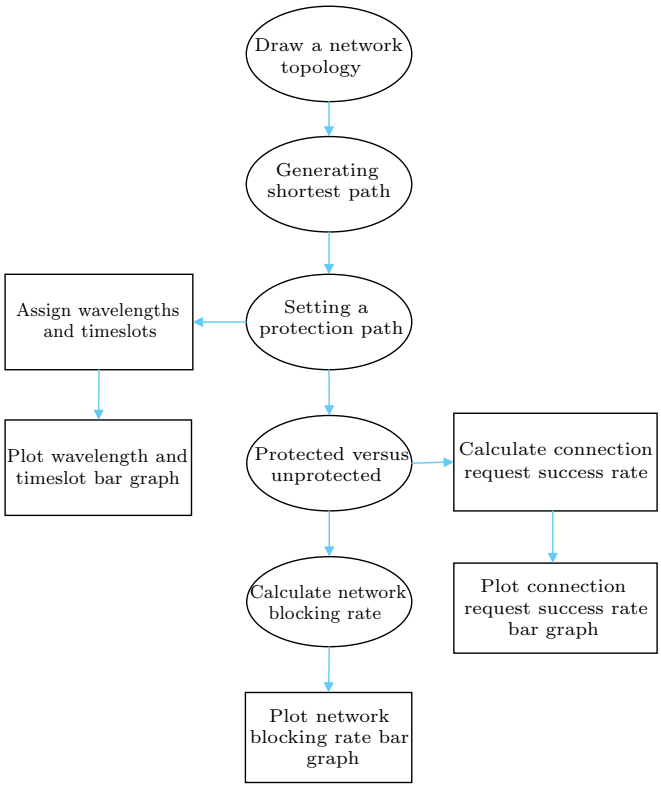


Fig. 4. Flowchart of protection path algorithm.

Therefore, the principles for establishing the protection path include: (i) the reliability and stability of the quantum link should be ensured when choosing the path, and the link with high loss or serious interference should be avoided as much as possible for the efficiency of key generation. (ii) the protection path should be independent of the main path to reduce the risk of single point failure. In addition to the initial and target nodes and the main path being the same, the nodes passing through the protection path cannot be duplicated with the main path to ensure that the protection path is different

from the main path. It is also necessary to consider the distribution of quantum relay stations to ensure that the signal can still be transmitted effectively at longer distances. (iii) the synchronization and key management of classical communication are reasonably arranged to realize fast switching between the main path and the protection path to ensure the security of the key and the continuity of the network. The specific flow chart of the protection path algorithm is shown in Fig. 4.

4.2. SM-RWTA algorithm

The blocking rate of optical networks is mainly triggered by wavelength and bandwidth competition, with a focus on bandwidth efficiency. While the blocking rate of QKD networks is more affected by security and real-time key updating and needs to prioritize the allocation of resources to safeguard the low-bit-error-quantum channel. At the same time, QKD network is subject to the additional constraints of photon loss and eavesdropping interference which leads to its blocking rate being usually higher and more dynamic. Each QKD request requires dedicated wavelengths and time slots for quantum and classical channels. As requests increase, resource contention arises, leading to blocking. The dynamic nature of key updates exacerbates this issue, necessitating efficient RWTA algorithms. Therefore, this paper proposes the SM-RWTA algorithm which aims to improve the security of QKD optical networks.

In QKD optical networks, the main reasons for blocking are resource allocation (during the initial SK of the request) and reallocation (during the SK update) of QKD optical path requests. QKD optical path requests are categorized into two types of optical path requests: high security metric requests (HSMRs) and low security metric requests (LSMRs), based on their security metric. QKD optical path requests with frequent SK updates and a higher security metric are called HSMRs, while QKD optical path requests with fewer SK updates and a lower security metric are called LSMRs. In the SM-RWTA algorithm, QKD optical path requests are serviced according to their priority order. The priority order of each QKD optical path request is based on the security metric. In other words, prioritize resource allocation to QKD optical path request HSMRs before any LSMRs in the network. A large amount of network resources will be served to the HSMRs with high security metric by utilizing prioritization. Therefore, the SM-RWTA algorithm can reduce the blocking of HSMRs in the network. In addition, the SM-RWTA algorithm can also reduce the overall blocking rate in the network. The reason is that updating the SK of HSMR requires a shorter key update period T_s, more updates N, and more resource reallocation compared to LSMR. The more frequent the key update, the less likely it is to be eavesdropped and deciphered. Thus, resource availability is essential in every QKD optical path request update. However, resources are allocated to a QKD optical path request without prioritization to serve the request in NSM-RWTA. Therefore, if the first requesting LSMR arrives at the network, the HSMR will have fewer resources during the reallocation period because the resources are allocated to the LSMRs in the network first. Thus, NSM-RWTA increases the blocking rate in the network. However, the HSMRs with high security metric will have the priority to be allocated resources and the LSMRs will also have enough resources to be allocated in the SM-RWTA algorithm due to security-metric-based prioritization. Thus, it can reduce the blocking rate in the network.

To explain the concept of blocking in QKD optical networks, we assume a network topology with five QCNs and seven QLs, as shown in Fig. 5. We consider that there are two QKD optical path requests (i.e., ac and ad) arriving at the network. The ac(LSMR) has a path length L of 1, a security level K of 3, and a security metric S of 3. The algorithm used is NSM-RWTA and the ad(HSMR) has a path length L of 2, a security level K of 8, and a security metric S of 4. The algorithm used is SM-RWTA.

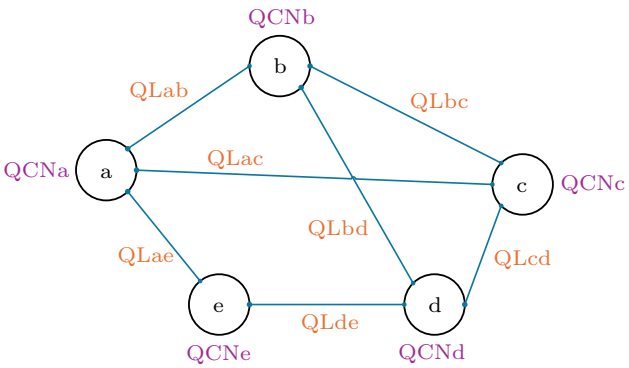


Fig. 5. Topology of five nodes and seven paths.

Assuming a QKD optical path request, the QLs consist of 20 time slots as shown in Figs. 6 and 7. We assume that a QKD optical path request ac(LSMR) arrives in the network with a route a–c from the source node QCNa to the destination node QCNc for the QKD optical path request ac(LSMR) and the path is QLac. ac(LSMR) requires three time slots for the initial key (SK) and four time slots for the update key (USK). First, the QKD optical path request ac(LSMR) searches for the availability of the required time slots in QLac. Since there are enough available time slots in the QLac for the initial SK of the ac, the ac is accepted during the time slot allocation, as shown in Fig. 6. During the SK update process, time slot reallocation is performed, and the ac searches for the availability of the required USK time slots in the QLac. Since there are enough available time slots for USK in QLac, they are allocated to ac (filled with green color) as shown in Fig. 6. As a result, the ac is accepted in the network.

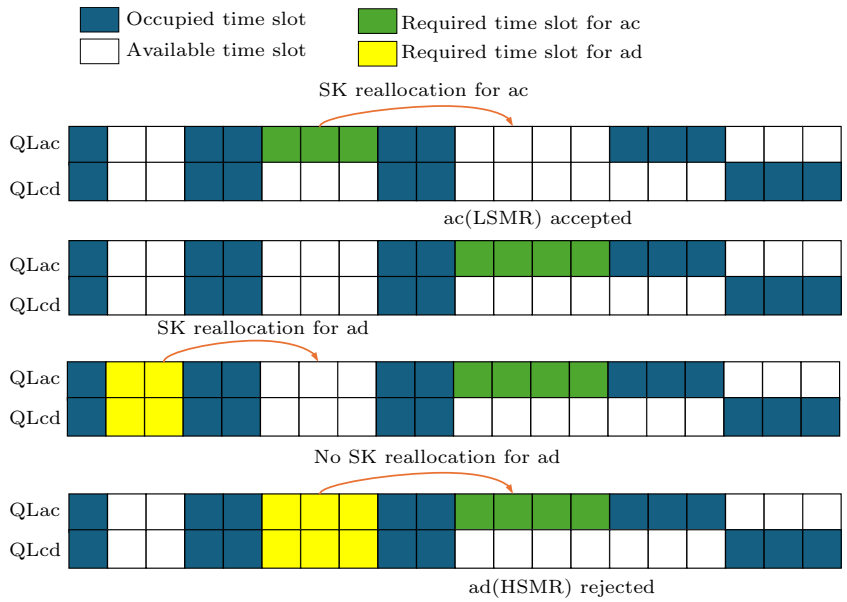


Fig. 6. Resource allocation and reallocation of NSM-RWTA.

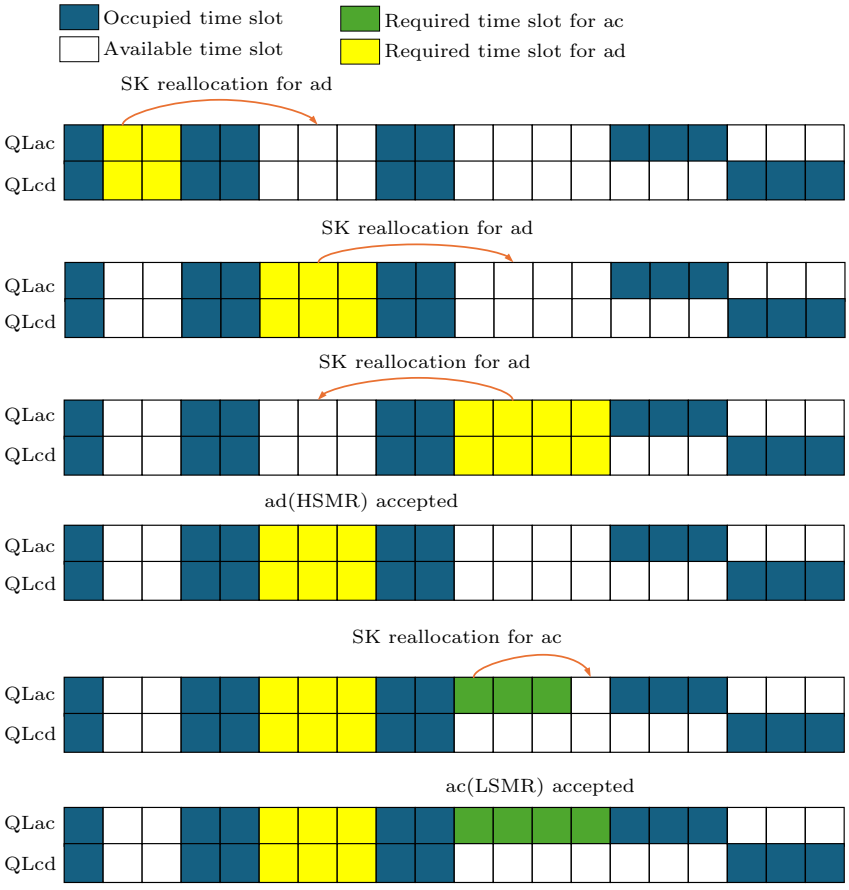


Fig. 7. Resource allocation and reallocation of SM-RWTA.

We assume that the ad(HSMR) arrives on the network. The optical path request ad(HSMR) is routed from the source node QCNa to the destination node QCNd as a–c–d. During resource allocation, the ad(HSMR) is accepted because there are available resources in the QLs: QLac and QLcd (populated in yellow), as shown in Fig. 6. However, during reallocation, there are not enough resources in QLac and QLcd to establish the connection between QCNa and QCNd. As a result, the ad(HSMR) is rejected when using the NSM-RWTA algorithm, which causes blocking.

To prevent blocking in the network, we propose a resource allocation strategy based on prioritization of the security metric. In the SM-RWTA algorithm, resources are prioritized to be allocated to HSMRs with a higher security met-

ric (S) so that the HSMRs are provided first in the network. From the example given above, it can be seen that the S value of QKD optical path request ad is greater than the S value of ac: $S_{ad} > S_{ac}$. Therefore, resources are first allocated to ad to establish a secure connection between QCNa and QCNd. To explain the concept of SM-RWTA, we consider that the requirements of QKD optical path request are the same as those of NSM-RWTA. In this case, the ad(HSMR) searches for the resource availability of the initial SK in the QLs. During the allocation process, the resources required by the ad are QLac and QLcd (filled with yellow color), as shown in Fig. 7.

To improve the security of the ad, the initial key (SK) needs to be updated three times, and a different time slot is required for each QKD optical path request update. During the reallocation process, the resources required for the ad (filled in yellow) are shown in Fig. 7 at each update. Therefore, ad(HSMR) can be accepted according to the proposed prioritization criteria. Similarly, ac(LSMR) is accepted during time slot allocation and reallocation because there are enough resources (filled with green color) in QLac as shown in Fig. 7. Using the security-metric-based algorithm, both QKD optical path requests (HSMR and LSMR) are accepted in the network. After all, the resources initially allocated to ad(HSMR) are available, and after the allocation and reallocation of ad(HSMR), there are also sufficient resources for ac(LSMR). This shows that the SM-RWTA algorithm can reduce the blocking rate of HSMR and improve the utilization of wavelengths and time slots in QKD optical networks.

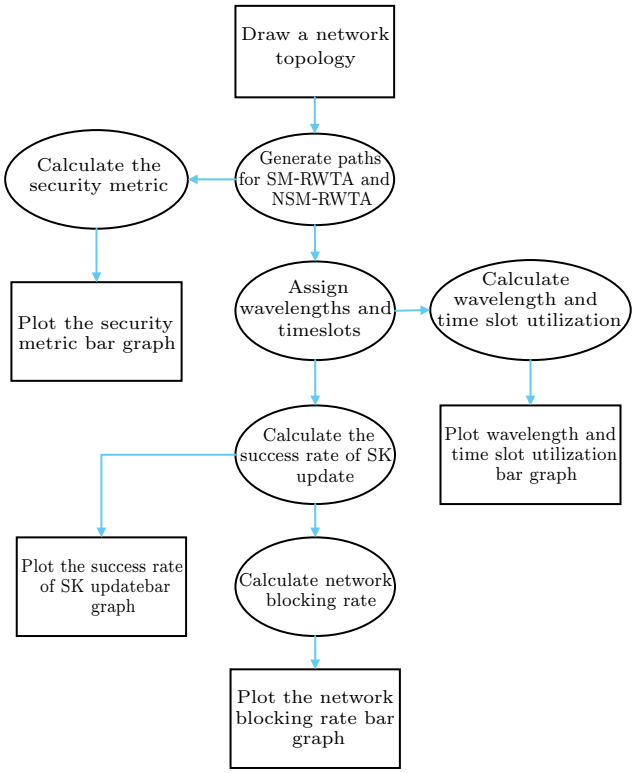


Fig. 8. Flowchart of SM-RWTA algorithm.

Therefore, the SM-RWTA algorithm is proposed based on the above analysis results of path requests allocation, and its specific algorithm process is shown in Fig. 8.

5. Simulation analysis

In this section, we analyze our proposed algorithm through simulation experiments. We use the National Science Foundation Network (NSFNET) topology with 14 nodes and 21 links for simulation, as shown in Fig. 9.

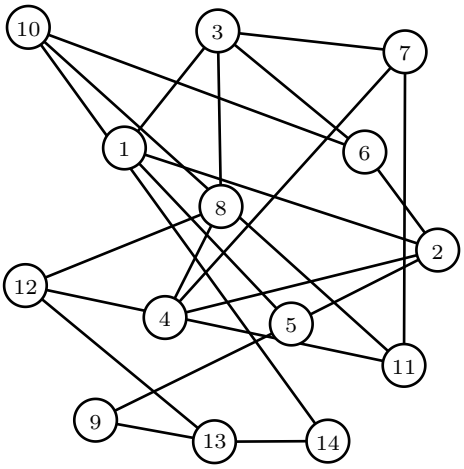


Fig. 9. Topology of 21 links for 14 nodes.

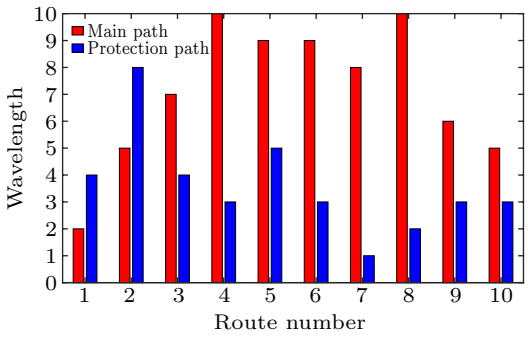


Fig. 10. Wavelength allocation for main and protection paths.

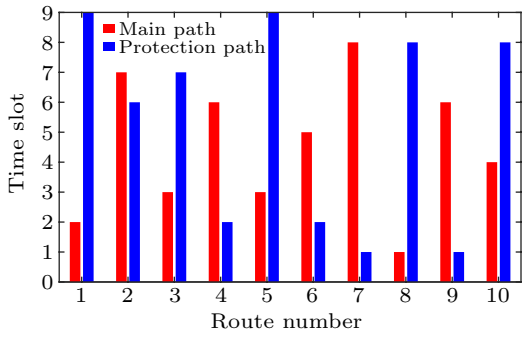


Fig. 11. Time slot allocation for main and protection paths.

We use the K shortest path algorithm to calculate the 10 shortest paths in the topology graph and set the wavelengths and time slots as 1–10. Then we assign them randomly to the 10 shortest paths, which are the main paths. After that, we set 10 protection paths for each of these 10 paths and ensure that the nodes of the paths are not the same as the main path, except

for the source node and the target node. This is to avoid the main path and protection path being the same, which would cause the protection path to be unprotected. Then we assign wavelengths and time slots to each of the 10 protection paths, as shown in Figs. 10 and 11. Wavelengths refer to the allocated wavelength channels in the optical network.

Firstly, the protection path algorithm is simulated and analyzed. We simulate the effects of external failures and disturbances on the network, and compare the success rates of connection requests between the network without protection path and the network with the protection path, as shown in Fig. 12, and the network blocking rate, as shown in Fig. 13. The simulation results show that the success rate of connection requests is higher, and the network blocking rate is lower in the network with the protection path. The protection effect is more significant with the increase of the request numbers, which indicates that the protection path can effectively protect the network and improve the ability of the network to cope with interference.

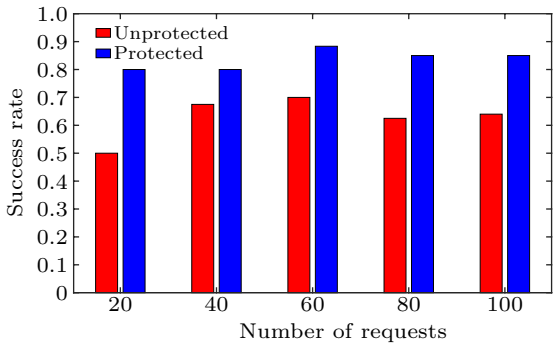


Fig. 12. Comparison of connection request success rate between the networks with and without protected path.

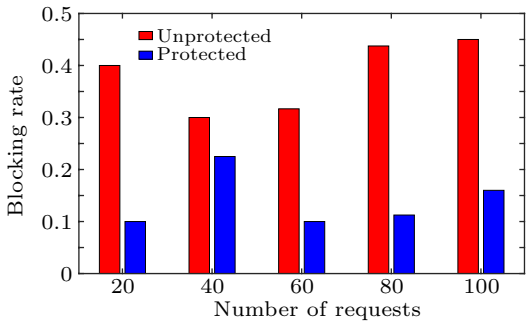


Fig. 13. Comparison of network blocking rate between the networks with and without protected path.

Meanwhile, we analyze the SM-RWTA algorithm and the NSM-RWTA algorithm in a comparative simulation in several dimensions. As shown in Fig. 14, the security metric of SM-RWTA is always higher than that of NSM-RWTA according to the comparative simulation analysis. That is because the SM-RWTA algorithm prioritizes requests with high security metric and allocates requests with high security metric, while NSM-RWTA gives resource allocation as soon as a request comes in without considering the security metric. In addition, we also control the variables by setting the number of hops N of the corresponding paths of both SM-RWTA and NSM-RWTA to a fixed value, so that the denominator of the security metric is fixed and only the effect of the security level K is considered, as shown in Fig. 15, which shows that the security metric of the SM-RWTA algorithm is consistently higher than that of NSM-RWTA. This is because even if the path lengths are the same, SM-RWTA can still take into account the priority order of security levels. Therefore, the security metric is still higher than that of NSM-RWTA.

Then we analyze the performance comparison between the SM-RWTA algorithm and the NSM-RWTA algorithm in terms of wavelength and time slot utilization, key update success rate and network blocking rate. The results are shown in Figs. 16–19. It can be seen that the SM-RWTA algorithm has a higher wavelength and time slot utilization than that of NSM-RWTA, a higher key update success rate than that of NSM-RWTA, and a significantly lower network blocking rate than that of NSM-RWTA. This is because the SM-RWTA algorithm has a security-metric-based prioritization criterion. The criterion is to prioritize the allocation of resources to HSMRs with high security metrics so that it can improve the utilization of resources such as wavelengths and time slots. The SM-RWTA algorithm can also effectively reduce the blocking rate in the network. Combined with the protection path, they improve the anti-interference ability and security of QKD optical networks by working together.

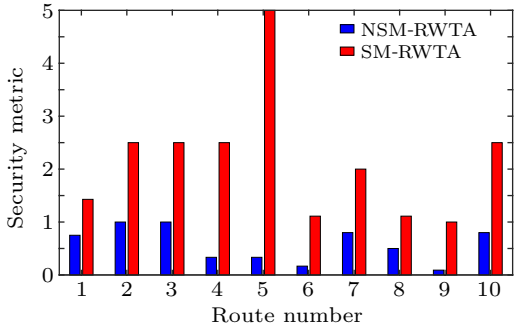


Fig. 14. Security metric of SM-RWTA and NSM-RWTA.

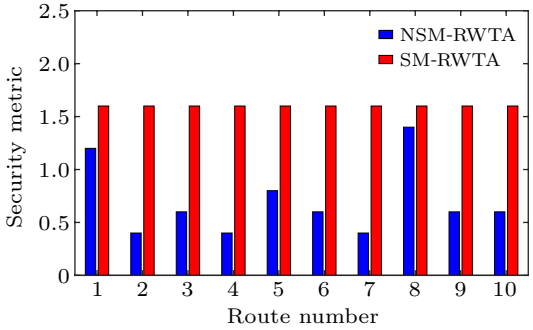


Fig. 15. Security metric of SM-RWTA and NSM-RWTA with fixed path lengths.

In order to further verify the conclusion, we also conducted a comparison experiment with priority order-based RWTA (POB-RWTA).[46] The results show that the SM-RWTA algorithm has a higher key update success rate and a

lower network blocking rate than the POB-RWTA algorithm. This is because the POB-RWTA algorithm only takes into account the effect of the security level whereas the security metric is more comprehensive as it considers the effects of security level and number of hops in the path.

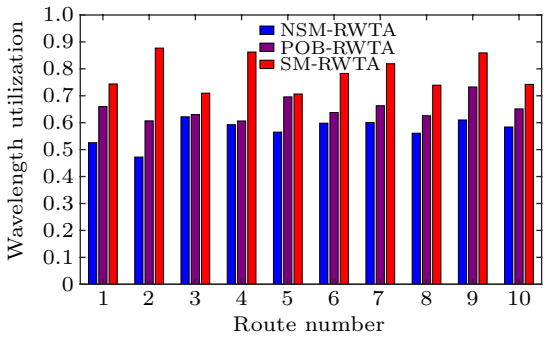


Fig. 16. Wavelength utilization of SM-RWTA, POB-RWTA and NSM-RWTA.

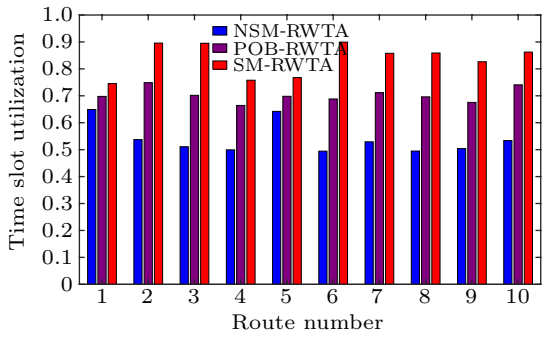


Fig. 17. Time slot utilization of SM-RWTA, POB-RWTA and NSM-RWTA.

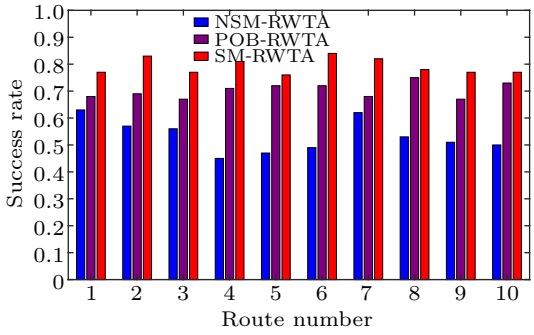


Fig. 18. Key update success rate of SM-RWTA, POB-RWTA and NSM-RWTA.

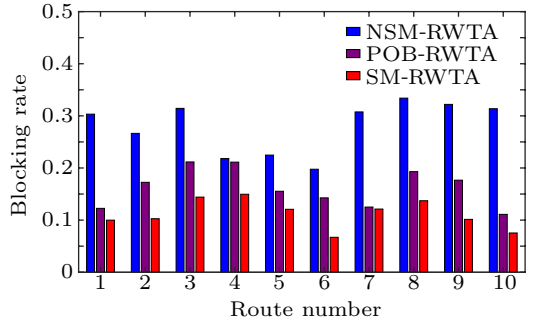


Fig. 19. Network blocking rate of SM-RWTA, POB-RWTA and NSM-RWTA.

6. Conclusion

Since QKD optical networks are always faced with interference and destruction from the outside world, their security has become an urgent problem to be solved. In this paper, we first propose a mechanism for the protection path. With QFC-based wavelength conversion technology, when the main path is blocked, the network can switch to the protection path to avoid network blockage. Simulation results show that the protection path can significantly improve the success rate of the network connection requests and enhance the anti-interference ability of QKD optical networks.

Then, the SM-RWTA algorithm is proposed in this paper to further improve the security of QKD optical networks. Through the simulation analysis of the SM-RWTA algorithm, the results show that the SM-RWTA algorithm performs better in terms of key update success rate, resource utilization and network blocking rate compared with the NSM-RWTA and POB-RWTA algorithms. It can be seen that the SM-RWTA algorithm can not only improve the success rate of key update, but also improve the resource utilization rate of wavelength and timeslot. Moreover, the SM-RWTA algorithm can also significantly reduce blocking in QKD optical networks and ultimately improve the security of the entire network.

The proposed algorithm demonstrates robust adaptability in dynamic networks through real-time priority adjustments of security metrics, ensuring efficient resource allocation under fluctuating conditions. Its polynomial-time complexity guarantees scalability for large-scale QKD deployments. However, limitations persist in long-distance scenarios due to increased path hops and key-rate constraints. Future work will focus on optimizing relay-node architectures and integrating quantum repeaters to extend applicability to global-scale quantum networks.

Acknowledgement

This research was funded by Youth Program of Shaanxi Provincial Department of Science and Technology (Grant No. 2024JC-YBQN-0630).

References

[1] Bi L, Yuan X T, Wu W J and Lin S X 2024 *Chin. Phys. B* **33** 030309
[2] Xu H X, Wang S H, Wang C L and Zhang P 2025 *Chin. Phys. Lett.* **42** 010303
[3] Zhang C X, Wu D, Cui P W, Ma J C, Wang Y and An J M 2023 *Chin. Phys. B* **32** 124207
[4] Brougham T and Oi D K L 2022 *New J. Phys.* **24** 075002
[5] Kaewpuang R, Xu M, Lim W Y B, Niyato D, Yu H, Kang J and Shen X 2023 *IEEE Internet of Things Journal* **11** 4454
[6] Muskan, Dutta A and Banerjee S 2025 *Phys. Scr.* **100** 055117
[7] You J, Wang Y and An J M 2021 *Chin. Phys. B* **30** 080302
[8] Rudavin N V, Gerasin I S, Mekhtiev E E, Duplinsky A V and Kurochkin Y V 2021 *J. Phys.: Conf. Ser.* **2086** 012098
[9] Ceylan O and Yilmaz I 2021 *IOP Conf. Ser.: Mater. Sci. Eng.* **1187** 012020

[10] Zhu Q, Yu X, Zhao Y, Nag A and Zhang J 2024 *IEEE Transactions on Network Science and Engineering* **11** 2153
[11] Olszewski I and Szcześniak I 2022 *Entropy* **24** 891
[12] Yang J W and Yang Y 2021 *J. Phys.: Conf. Ser.* **2132** 012020
[13] Chen Q H, Zhao Y, Li C and Li X 2023 *New J. Phys.* **25** 113045
[14] Liu H, Huo X, Chen Y, Qiu Y, Chen H, Chen X and Zhang J 2024 *Journal of Lightwave Technology* **42** 5800
[15] Gerstel O and Ramaswami R 2000 *IEEE Journal on Selected Areas in Communications* **18** 1885
[16] Somani A K and Vaidya N H 1997 *IEEE Computer* **30** 45
[17] Guo L, Cao J, Yu H and Li L 2006 *Journal of Lightwave Technology* **24** 1129
[18] Wei D, Guo Y and Luo J W 2021 *J. Phys.: Conf. Ser.* **1856** 012044
[19] He B, Ma W K, Chen H, Shao W D, Gao M Y, Chen B W and Wu J B 2022 *Asia Communications and Photonics Conference (ACP)*, 05–08 November 2022 Shenzhen China pp. 1196–1198
[20] Wang Y H, Yu X S, Li J C, Zhao Y L, Zhou X T, Xie S M L and Zhang J 2019 *Asia Communications and Photonics Conference (ACP)*, 02–05 November 2019 Chengdu, China, pp. 1–3
[21] He B, Lu Y X, Chen H, Shao W D, Jiang M, Zhou L L, Chen B W and Ju W G 2023 *Asia Communications and Photonics Conference/2023 International Photonics and Optoelectronics Meetings (ACP/POEM)*, 04–07 November 2023 Wuhan, China, pp. 1–3
[22] Zhang P and Mao X J 2020 *J. Phys.: Conf. Ser.* **1621** 012017
[23] Kravtsov K S 2023 *Laser Phys. Lett.* **20** 085203
[24] Lasota M, Kovalenko O and Usenko V C 2023 *New J. Phys.* **25** 123003
[25] Reutov A, Tayduganov A, Mayboroda V and Fat'yanov O 2023 *Entropy* **25** 1556
[26] Zheng Y, Shi H B, Pan W, Wang Q T and Mao J H 2022 *Entropy* **24** 127
[27] Xu S J, Li Y, Wang Y J, Mao Y, Wu X D and Guo Y 2021 *Entropy* **23** 1698
[28] Sharma P, Bhatia V and Prakash S 2020 *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 14–17 December 2020 New Delhi, India, pp. 1–6
[29] Wen B, Shenai R and Sivalingam K 2005 *Journal of Lightwave Technology* **23** 2598
[30] Wen B and Sivalingam K M 2002 *Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, 23–27 June 2002 New York, NY, USA, pp. 1442–1450
[31] Cao Y, Zhao Y L, Yu X S and Wu Y 2017 *Journal of Optical Communications and Networking* **9** 995
[32] Cui W, Yang C, Huang G Q and Jiao R Z 2024 *Phys. Scr.* **99** 085112
[33] Ma W K, Chen B W, Liu L, Chen H, Shao W D, Gao M Y, Wu J B and Ho P H 2022 *IEEE Internet of Things Journal* **9** 25660
[34] Yang C and Jiao R Z 2025 *Phys. Scr.* **100** 045106
[35] Ma H Q, Han Y X, Dou T Q and Li P Y 2023 *Chin. Phys. B* **32** 020304
[36] Sych D, Duplinskiy A and Babukhin D 2021 *J. Phys.: Conf. Ser.* **1984** 012001
[37] Navarrete A and Curty M 2022 *Quantum Sci. Technol.* **7** 035021
[38] Feng B, Huang H D, Bian Y X, Jia W, Zhou X Y and Wang Q 2023 *Chin. Phys. B* **32** 030307
[39] Cui W, Yang C, Huang G Q and Jiao R Z 2024 *Phys. Scr.* **99** 085112
[40] Sun S J, Wang J P, Su D and Ma H Q 2022 *J. Phys.: Conf. Ser.* **2381** 012082
[41] Sun Z Q, Han Y X, Dou T Q, Wang J P, Li Z H, Zhou F, Huang Y Q and Ma H Q 2021 *Chin. Phys. B* **30** 110303
[42] Kiselev F, Veselkova N, Goncharov R and Egorov V 2021 *J. Phys. B: At. Mol. Opt. Phys.* **54** 135502
[43] Harkness A, Krawec W O and Wang B 2025 *Quantum Sci. Technol.* **10** 015005
[44] Ma W, Liu L, Chen B, Gao M Y, Chen H and Wu J B 2020 *Asia Communications and Photonics Conference (ACP) and International Conference on Information Photonics and Optical Communications (IPOC)*, 24–27 October 2020 Beijing, China pp. 1–3 h
[45] Doai R, Hayashi R, Matsukawa T, Seki T, Miyamura T and Kawabata A 2025 *IEICE Communications Express* **14** 2187
[46] Sharma P, Bhatia V and Prakash S 2020 *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 14–17 December 2020 New Delhi, India, pp. 1–6
[47] Cao Y, Zhao Y L, Yu X S, Wang H, Liu C, Li B L and Zhang J 2017 *Opto-Electronics and Communications Conference (OECC) and Photonics Global Conference (PGC)*, 31 July 2017–04 August 2017 Singapore, pp. 1–3
[48] Gowda S and Sivalingam K M IEEE INFOCOM 2003 *Twenty second Annual Joint Conference of the IEEE Computer and Communications Societies*, 30 March 2003–03 April 2003 San Francisco, CA, USA pp. 12–21