Quantum Communication Network Routing With Circuit and Packet Switching Strategies

Ze-Zhou Sun, Yuan-Bin Cheng, Dong Ruan, Dong Pan, *Member, IEEE*, Fei-Hao Zhang, and Gui-Lu Long, *Member, IEEE*

***Abstract*— Quantum network extends the ability to transmit information securely from two-party communication to multi-party communication with arbitrarily long distances. The efficiency of secure communication in a quantum network depends on both the topology of the network and the strategy of communication relays. In this paper, we propose a strategy to build a quantum network integrating various types of quantum secure direct communication (QSDC) schemes. A cost optimization model is presented to measure the cost of transmitting secure messages in a quantum network. Within the model, two types of quantum network strategies, the quantum circuit switching strategy and the quantum packet switching strategy, are proposed and compared. Numerical simulations in a specific network show that the quantum packet switching strategy is more favorable in future quantum networks taking into account robustness and cost required when using different types of QSDC schemes.**

***Index Terms*— Quantum communication network, circuit switching, packet switching, optical network, quantum secure direct communication.**

Received 21 March 2024; revised 30 August 2024; accepted 11 November 2024. Date of publication 19 February 2025; date of current version 14 May 2025. The work of Dong Ruan was supported by the National Natural Science Foundation of China under Grant 62131002. The work of Dong Pan was supported in part by the National Natural Science Foundation of China under Grant 12205011 and in part by the Open Research Fund Program of the State Key Laboratory of Low-Dimensional Quantum Physics under Grant KF202205. The work of Gui-Lu Long was supported in part by the National Natural Science Foundation of China under Grant 11974205, in part by the Key Research and Development Program of Guangdong Province under Grant 2018B030325002, in part by Beijing Advanced Innovation Center for Future Chip (ICFC), in part by Tsinghua University Initiative Scientific Research Program, and in part by the Open Research Fund Program of the State Key Laboratory of Low-Dimensional Quantum Physics under Grant KF202205. *(Ze-Zhou Sun and Yuan-Bin Cheng are co-first authors.) (Corresponding authors: Dong Pan; Fei-Hao Zhang; Gui-Lu Long.)*

Ze-Zhou Sun and Yuan-Bin Cheng are with Beijing Academy of Quantum Information Sciences, Beijing 100193, China, and also with the State Key Laboratory of Low-Dimensional Quantum Physics and the Department of Physics, Tsinghua University, Beijing 100084, China (e-mail: szz21@mails.tsinghua.edu.cn; chengyb21@mails.tsinghua.edu.cn).

Dong Ruan is with the State Key Laboratory of Low-Dimensional Quantum Physics, the Department of Physics, and the Frontier Science Center for Quantum Information, Tsinghua University, Beijing 100084, China (e-mail: dongruan@tsinghua.edu.cn).

Dong Pan and Fei-Hao Zhang are with Beijing Academy of Quantum Information Sciences, Beijing 100193, China (e-mail: pandong@baqis.ac.cn; zhangfh@baqis.ac.cn).

Gui-Lu Long is with the State Key Laboratory of Low-Dimensional Quantum Physics, the Department of Physics and the Frontier Science Center for Quantum Information, Tsinghua University, Beijing 100084, China, and also with Beijing Academy of Quantum Information Sciences, Beijing 100193, China (e-mail: gllong@mail.tsinghua.edu.cn).

Digital Object Identifier 10.1109/JSAC.2025.3543524

I. Introduction

QUANTUM secure direct communication (QSDC) [1], proposed in 2000, directly transmits confidential information using quantum states without first negotiating secret keys. It is different from quantum key distribution (QKD) [2], which negotiates secure keys among two distant users, and messages are transmitted by using classical communication of the ciphertext of classical cryptography [3], [4].

Quantum networks, as a new type of information processing and connecting method, have great potential in realizing various applications with information transmission and encryption in multi-user scenarios [5]. They have become one of the most important directions of quantum information technology [6]. Practical quantum networks require a specific method of device deployment. Different repeaters can be deployed to build quantum networks, and the security they provide varies. Meanwhile, the cost is also a concern, since the quantum technology necessitates novel designs that differ from its classical counterpart. Therefore, it is essential to consider a deployment method that meets current technical security standards while minimizing costs. One way to address this issue is to introduce secure repeaters and untrusted repeaters when deploying quantum networks. Secure repeaters are proposed as a component of a secure repeater network (SRN) [7], which relies on QSDC to transmit ciphertext generated by cryptographic algorithms [8] and classical relaying. Deploying untrusted repeaters is one way to implement the measurement-device-independent QSDC (MDI-QSDC) scheme [9], [10], [11], which enables secure communication over an extended point-to-point range. Both secure and untrusted repeaters are realistic solutions for building quantum networks that comply with current security standards. Since an untrusted repeater requires that both of its ends be secure in the MDI-QSDC, there is a limit to the distance that can be extended solely using untrusted repeaters. The limit is necessary to ensure communication security. However, practical quantum networks often require longer communication distances. Hence, to ensure security in a practical quantum network, the communication distance cannot be further extended by other untrusted repeaters at either end of an untrusted repeater. Secure repeaters can be deployed at the endpoints of untrusted repeaters to guarantee security and prolong communication distance. Consequently, embedding untrusted repeaters in a quantum network necessitates the simultaneous embedding of secure repeaters. It is necessary to study QSDC networks

© 2025 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License.
For more information, see https://creativecommons.org/licenses/by/4.0/

that employ a hybrid deployment of untrusted and secure repeaters.

In classical networks, there are two major methods of data exchange between two servers, circuit switching (CS) and packet switching (PS) [12]. The CS strategy requires that a connection be established first before the communication, and it is released after the communication is completed [13]. The PS service does not require the establishment of an end-to-end connection [14]. Classical data exchange strategies have been developed relatively mature [15], [16], however, switching strategies for quantum communication have not yet been thoroughly studied. Recently, some scholars have envisioned the importance of studying the two strategies in quantum networks, pointing out that the future design of quantum Internet requires a major paradigm shift for harnessing the unique characteristics of quantum information [17]. Although packet switching strategies have been favored in classical networks in recent years, due to the scarcity of quantum resources, establishing a unicast-dedicated channel between a pair of nodes has also been necessary [18], [19]. At the same time, the quantum network demands tight synchronization and signaling [17], which may result in an increased need for pre-established connections. To better integrate with existing classical networks and consider the fundamental differences between quantum and classical communication, it is essential to develop and compare quantum network communication strategies for efficient and convenient information transmission.

In this paper, two types of quantum network strategies are proposed and we also present a method for hybrid deployment of untrusted relays and secure relays, as well as discuss its cost issues. Our main contributions are summarized as follows:

- We propose a QSDC network implementation and architecture of hybrid deployment with secure repeaters and untrusted repeaters and explain the network operating mechanism.
- We propose a quantum circuit switching strategy that establishes a stable connection between any two nodes in a QSDC network. We also propose a quantum packet switching strategy with which secure messages can be transmitted without the need for a pre-existing connection.
- We propose a cost estimation model specifically tailored for hybrid QSDC networks integrated within existing optical infrastructure. These networks are designed with a hybrid deployment strategy, incorporating both untrusted repeaters and secure repeaters. Additionally, we introduce a heuristic routing algorithm to optimize the overall cost of the hybrid QSDC network deployment.
- We assess the performance of the algorithm via dynamic network simulations that encompass the establishment and termination of connections over a period of time. Furthermore, we conduct a comprehensive comparative analysis of key network parameters within the context of hybrid QSDC networks.

The rest of this paper is organized as follows. Section II demonstrates the basic architecture and node structure of the QSDC network. In Section III, two types of strategies to deliver secure messages are proposed. Section IV develops the cost model of the QSDC network and an algorithm is proposed to decide the route for different strategies. The simulation results in specific networks with different infrastructures are given in Section V. Finally, Section VI gives the conclusion.

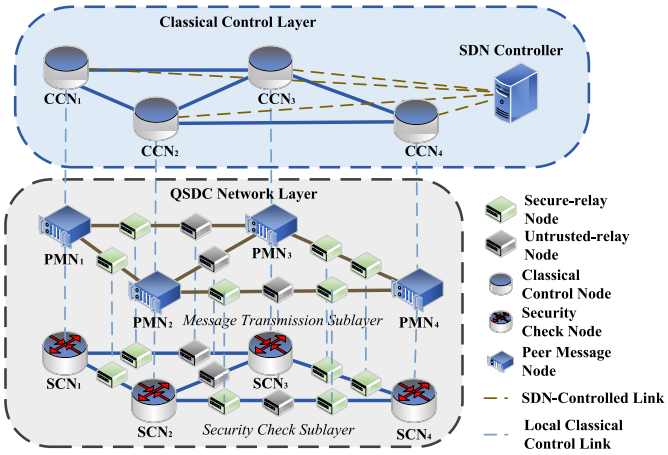

Fig. 1. Architecture implementation diagram of QSDC network. CCN represents the classical control node, PMN represents the peer message node, and SCN represents the security check node.

II. QSDC Network Architecture

SRN, which serves as an intermediate stage toward the ultimate fully-fledged quantum internet, is compatible with the operational Internet [7]. Explicitly, in the SRN, the ciphertext gleaned from a quantum-resistant algorithm is transmitted using QSDC along the nodes, where it is read out and then transmitted to the next node. At the same time, the security check in QSDC is also important in the secure transmission of information [20]. In these processes, both classical information and quantum information play roles in the network. In this section, we study the implementation, architecture design, and logical layering of the QSDC network.

Our QSDC network architecture is divided into the classical control layer and the QSDC network layer as shown in Fig. 1. The blue dashed lines represent the links utilized for classical communication between the local devices, whereas the brown dashed lines signify the links for classical communication between the software-defined network (SDN) and the classical control nodes. In the classical control layer, the SDN controller [21] supervises the overall situation of the network in real-time. It also controls and manages the classical control node to allocate network resources, which will be discussed in Section III. Classical control nodes directly interact with the nodes of the QSDC network layer. The QSDC network layer can be divided into the message transmission sublayer and the security check sublayer. These two sublayers achieve information-theoretic secure communication together and the encrypted information is transmitted through quantum channels. It should be noted that this is significantly different from the classical optical network layer of QKD networks [22], [23]. In the QKD network, after the QKD layer negotiates the key, the encrypted information needs to be transmitted via the classical optical network [24]. By contrast, the QSDC network

directly uses the message transmission sublayer to transmit encrypted information, and the security check sublayer only exchanges a small amount of photons and classical information for the security check.

Nodes in the message transmission sublayer, responsible for transmitting quantum information, play a pivotal role in the entire QSDC network. There are three types of nodes used for realizing the transmission of quantum information, namely peer message nodes, secure-relay nodes, and untrusted-relay nodes. Peer message nodes serve as endpoints that can generate communication requests, route messages, as well as read encrypted information. Secure-relay nodes and untrusted-relay nodes facilitate the relay of information between peer message nodes. Notably, peer message nodes are legitimate secure endpoints, while secure-relay nodes, though potentially subject to eavesdropping, are designed not to leak private information [7]. By contrast, the measurement devices of untrusted-relay nodes may be controlled by potential eavesdroppers [9], [10], [11].

Then, we discuss how the point-to-point communication schemes operate within our network nodes. Typical QSDC schemes, such as the DL04 protocol [20], quantum-memory-free (QMF) QSDC scheme [25], etc., can be employed to achieve information-theoretically secure communication between two directly connected secure endpoints. In the subsequent discussion of this paper, we will take the DL04 scheme as an example for our study. However, it is important to note that the architecture, devices, and algorithms mentioned in this paper are also applicable to other conventional QSDC schemes, including the QMF scheme, and multi-intensity QSDC scheme [26]. MDI-QSDC schemes [9], [10], [11] can overcome security loopholes caused by imperfect detectors. It enables secure communication between two parties, even when the quantum measurement is conducted by an untrusted third-party in the middle of the two communication parties. However, in terms of communication security, two untrusted nodes cannot be directly connected for a wider range of communication.

Fig. 2 shows the specific node structures of the secure repeater and the untrusted repeater. Secure repeaters are set in peer message nodes and secure-relay nodes, while untrusted repeaters are set in peer message nodes and untrusted-relay nodes. It should be noted that peer message nodes not only play the role of relaying, but also the role of interacting with the client and performing quantum-resistant cryptography encryption on the messages to be transmitted.

An untrusted repeater contains the MDI-QSDC detector that can perform Bell-state measurement (BSM) and the single-photon measurement device which is actually a conventional QSDC detector, as shown in Fig. 2a . Untrusted-relay nodes must be connected to secure-relay nodes or peer message nodes to achieve secure transmission of messages. When photons are transmitted to the untrusted-relay node through the quantum channel and demultiplexed, the optical switch controls the photons to enter the MDI-QSDC detector or conventional QSDC detector. This is related to the MDI-QSDC process [9]. Specifically, in MDI-QSDC, two rounds of photon transmission are required. During the first transmission, two adjacent ends each transmit photons to the untrusted third party for BSM. The untrusted third party also performs single photon measurements after the second round of transmission. Therefore, a complete MDI-QSDC process will use the MDI-QSDC transmitters three times, the MDI-QSDC detector one time, and the conventional QSDC detector one time.

Secure-relay nodes can be deployed next to peer message nodes, other secure-relay nodes, or untrusted-relay nodes. A secure repeater contains a conventional QSDC detector, a conventional QSDC modulator, a conventional QSDC transmitter, and an MDI-QSDC transmitter, as shown in Fig. 2b. Demultiplexed photons can switch paths using the optical switches. If the secure-relay node is connected to the peer message node or another secure-relay node, the repeater first uses the conventional QSDC transmitter to transmit random photons to the previous node. After the encoded photon is sent back to the repeater, the ciphertext is read by the detector and then transmitted to the next node by the conventional QSDC modulator. This is related to the DL04 process [20]. Specifically, in DL04, two rounds of photon transmission are required. During the first transmission, the message receiver transmits random photons to the sender. After the message sender confirms that the channel is secure, the message is encoded on these random photons and transmitted back to the receiver for measurement. Therefore, a complete DL04 process will use the conventional transmitter one time, the conventional detector one time, and the conventional QSDC modulator one time. If the secure-relay node is connected to an untrusted-relay node, the read ciphertext will be transmitted by an MDI-QSDC transmitter to another peer message node or secure-relay node.

In the process of security check, the erbium-doped fiber amplifiers can also be deployed at the positions corresponding to the secure-relay nodes and untrusted-relay nodes to amplify classical signals. Combined with wavelength-division multiplexing technology [27], quantum signals and classical signals can be multiplexed in the same optical fiber using multiplexing and demultiplexing (MUX/DEMUX) devices [28], [29]. In addition, $100\,\mathrm{km}$ QSDC has been implemented experimentally [7]. Thus, we should deploy a repeater within a distance of $100\,\mathrm{km}$ and it is necessary to deploy repeaters within shorter distances for better communication effects.

III. Quantum Circuit Switching and Packet Switching Strategies

In this section, we exhibit two quantum network strategies for achieving secure information transmission in the QSDC network. The strategies we are discussing are of two types, one of which relies on quantum circuit switching, while the other relies on quantum packet switching. We suppose that the nodes in the QSDC network forward packets in the same route that the SDN has given when the classical communication between the SDN and every node is provided. We also suppose that the classical network for broadcasting classical messages is reliable [30].

It should be noted that the ″node″ in this section is different from the one in Sec. II. It is a logical node used for driving

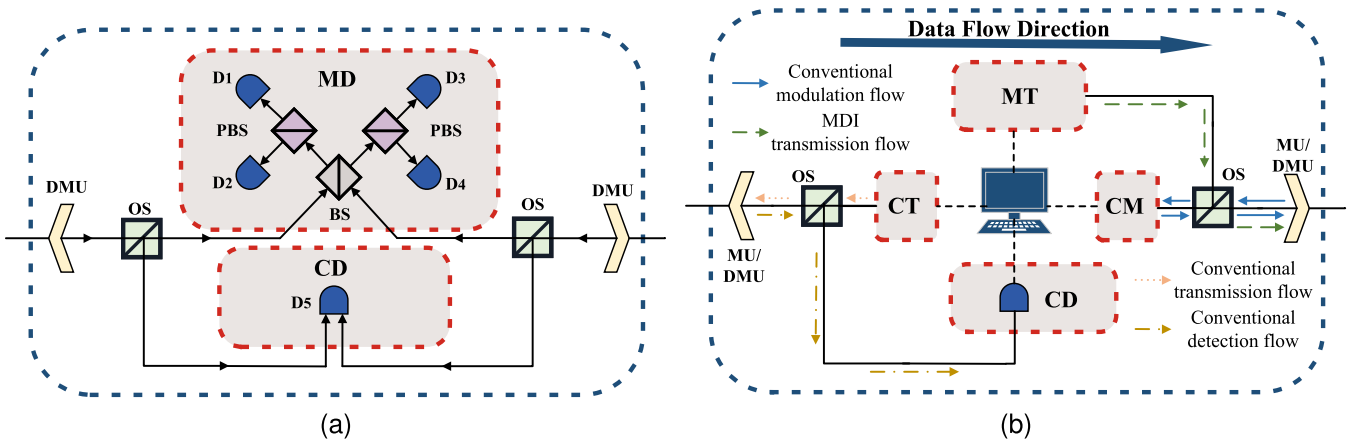

Fig. 2. Schematic diagram of repeaters in peer message nodes, secure-relay nodes and untrusted-relay nodes. (a) Untrusted repeater. (b) Secure repeater. CD represents the conventional QSDC detector, CT represents the conventional QSDC transmitter, CM represents the conventional QSDC modulator, MT represents the MDI-QSDC transmitter, MD represents the MDI-QSDC detector, OS represents the optical switch, PBS represents the polarizing beam splitter, BS represents the beam splitter, D represents the detector, and MU/DMU represents the multiplexer and demultiplexer device.

corresponding functions. Here, every node in the quantum network can be uniquely identified by an attribute, address. The addresses of different nodes are different. We will call the node that sends out a secure message the source node and the node that receives the secure message the destination node. Their addresses are the source address and destination address, respectively. Suppose that the secure messages can be transmitted between nodes connected by a link in the quantum network. This can be realized by the conventional QSDC scheme or the MDI-QSDC scheme when the secure-relay nodes or untrusted-relay nodes are appropriately deployed on the link. Additionally, suppose that the classical communication between a node and the SDN is supported. Every link in the quantum network has an attribute called capacity, which is known to the nodes that it connects and the SDN. Every node in this section can be regarded as a collection of the peer message node, the classical control node, and the security check node that are at the same location. The secure transmission between connected nodes can be realized by communication between the connected security check nodes and between the connected peer message nodes. The classical communication with the SDN is implemented in classical control nodes. The resource mentioned in the section is the available capacity, which can be used to transmit secure messages between connected nodes.

A. Quantum Packet Switching Strategy

The quantum packet switching strategy is the one that is used to send a message from one node to another directly with the route given by the SDN. The SDN can control the route directly or indirectly.

When a quantum network adopts the indirect strategy, the SDN will initialize the network by setting a series of rules for each node in the quantum network. These rules will tell the nodes how to handle received packets. Specifically, the nodes will forward packets according to the tables that the SDN sends to them. It is similar to the forwarding table in the classical network [31]. After a node receives a packet, it will read the header of the packet and look up the table to find to which port it forwards the packet. Here, we consider a destination-based forwarding. The header of the packet needs to contain the destination address and the required capacity. After the SDN initializes the quantum network, communication using the quantum packet switching strategy can begin. The source node encapsulates its secret message with a header containing the destination address and required capacity to form a packet. The packet is transmitted to the next node according to the rules that the SDN has set. The secret message is transmitted as quantum states to ensure security while the header is transmitted classically. After the next node receives the packet, it will read the header to decide to which port to forward so that the subsequent node on the route can receive the packet if the resource is enough. Otherwise, it will abort the packet. If the packet is forwarded by every node on the route, it will arrive at the destination node and the packet delivery is completed. The abortion of packets will be recorded by nodes and the SDN will be informed by classical communication with nodes. The SDN can adjust rules according to the abortion signals and change the tables of nodes by classical communication with them.

The direct control requires that the source node sends a transmission request to the SDN before sending out the packet. The transmission request contains the destination address and required capacity. The SDN decides whether the packet can be transmitted to the destination node. If it is possible, the SDN gives the route and updates the table of the nodes, including the source node and the destination node, on the route. Then, the SDN responds to the transmission request with permission. After the source node gets the permission, the source node sends out packets according to the updated table. The transmission of packets between connected nodes is the same as the one in the indirect strategy. That is, the node that sends out packets first encapsulates the secret message with a header to form a packet and the packet will be transmitted by encoding into quantum states and classical signals. The node that receives the packet will forward the packet according to the header unless the node is the destination node. If the SDN

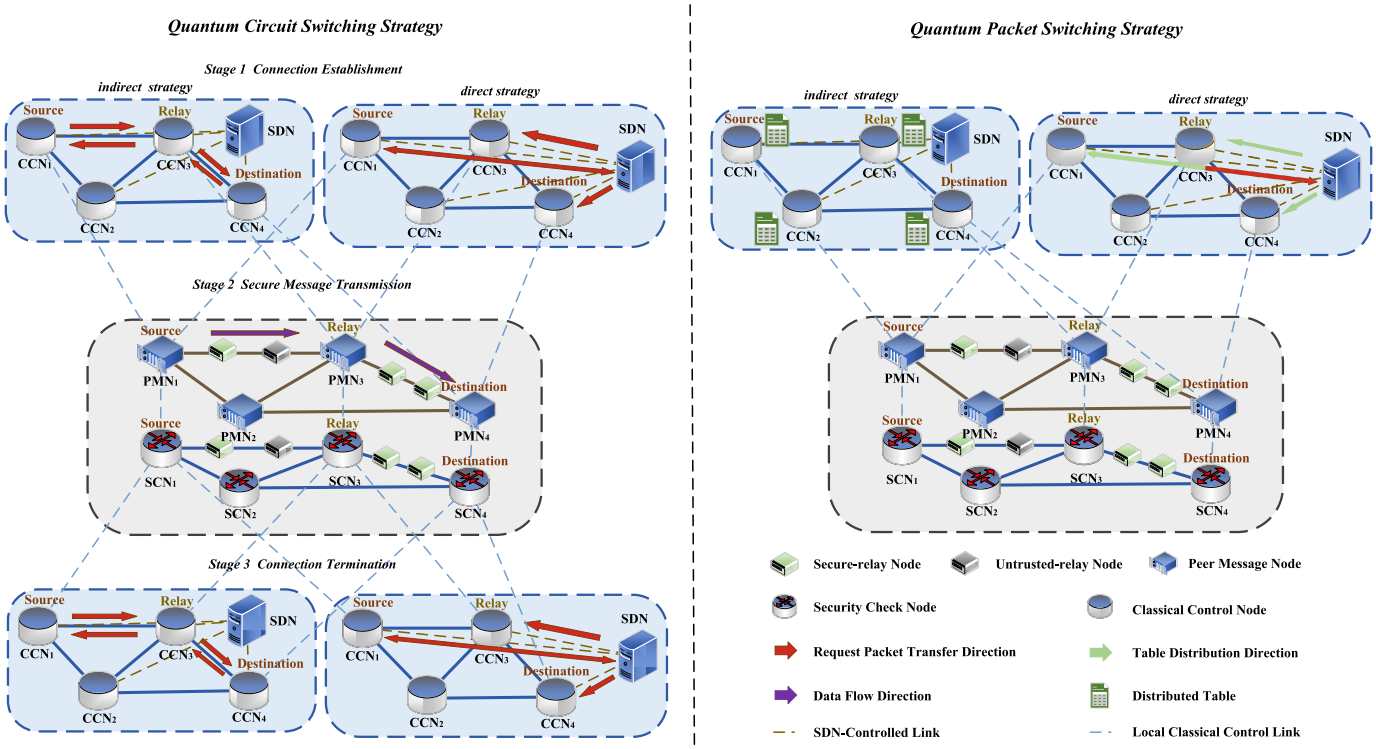

Fig. 3. Flowchart for information transmission using quantum circuit switching and quantum packet switching strategies.

denies the transmission request, the SDN will respond to the transmission request with a denial. After the source node gets the denial, it should give up sending out the packet.

B. Quantum Circuit Switching Strategy

Quantum circuit switching strategy requires first establishing a connection between two communicating nodes, which is a dedicated end-to-end connection. After the connection is built, the source node can send the secure messages. A termination signal that is sent by the source node or the destination node will be broadcast to every node on the route to release the resources that the connection occupies. The three steps using the quantum circuit switching strategy are shown in Fig. 3.

1) Connection Establishment: The purpose of connection establishment is to make sure that the destination node can receive and deal with the messages sent by the source node. We also give two strategies, the indirect one and the direct one, to establish the connection.

In the indirect one, the source node sends out a packet without a payload. The route is along the nodes that forward the packet after they read the header of the packet, which is shown in Fig. 4. It should be noted that the address in the header is classical and can be stored in a classical register. The address is different from that in Ref. [32], where a quantum addressing is given. The label is the index of the connections initialized by the source node. The first flag indicates the direction of the packet delivery. A certain value of the second flag labels whether connection establishment has been denied.

Classical Packet	**Source Address**	**Destination Address**
	Capacity Requirement	
	Label	
	Flag 1 - Direction	**Flag 2 - Denial**

Fig. 4. Data structure diagram transmitted by the indirect method of connection establishment in the quantum circuit switching strategy.

After the destination node receives the packet, it changes the value of the second flag. Then, the destination sends back the packet. The nodes on the route recognize the reception by the changed first flag and the unchanged second flag. After the source node receives the packet, the connection has been established. To send the denial, a node changes the first flag to reverse the delivery and changes the second flag to indicate the denial. The memory associated with the connection will be reset by the nodes that receive the denial.

In the direct one, the source node sends a connection-establishment request, which contains the source address, destination address and capacity requirement, to the SDN. Then, the SDN asks the destination node whether to accept the connection. After receiving the agreement of the destination node, the SDN computes the route according to the routing algorithm discussed in Section IV. The SDN updates nodes' tables and sends the messages with the required capacity, source address and connection label to the nodes on the route

if there is a route that satisfies the capacity requirement. Otherwise, the SDN sends a denial to the source node.

Because classical headers do not carry the secret information of the communication during the connection establishment process, the eavesdropper will not get useful information. Besides, in order to ensure the information-theoretic security of establishing a connection, it is also feasible to use quantum channels to complete this process, but this will increase the cost in practical applications.

2) Secure Messages Transmission: After a connection between the source node and the destination node is established, the transmission can be performed. The source node packages the header and the secure messages into a packet. The secure message will be transmitted as quantum states and the header will be transmitted classically. The subsequent nodes then decode these signals into classical messages and read the header to acquire information to decide to which node they forward the packet. It should be noted that the secure message is encrypted by a quantum-resistant algorithm [7]. Then, the nodes encode the secure messages into quantum states and the header into classical signals, which will be transmitted to the next nodes. After the destination node receives the packet, it decodes these signals into the classical message. To transmit more messages, the source node needs to create more packets to deliver in the same way described above.

3) Connection Termination: As in the part of connection establishment, there are two strategies to inform every node on the route.

In the indirect one, where the connection is established by transmitting a packet along the route, the closing is similar. The node that wants to terminate the connection sends a denial to the nodes on the routes.

In the direct one, where the connection is established by communication with the SDN, the node that decides to close the connection sends a connection-closing request to the SDN with the label of the connection and the source address. Then the SDN sends connection-closing requests to every node on the route and updates the resource information of the quantum network.

The reliability of the transmission of the classical message ensures that every classical message sent by the SDN or the nodes on the route will be received, and hence the resource can be released as expected.

IV. Network Cost-Based Control

In quantum networks, routing selection has an important impact on the exploitation of rare quantum resources. Selecting the best routing method relying on the actual situation of network resources can also help alleviate network congestion. In this section, we propose a routing algorithm to decide the path of transmission in the quantum network according to a cost model.

A. Network Cost Model

We first elaborate on the cost model of deploying a hybrid QSDC network with secure- and untrusted-relay nodes on the existing optical network. It should be noted that the cost comes from various network components that need to be deployed to support QSDC and is calculated as the usage cost of each device for a single transmission.

1) Cost of Transmitter, Receiver, and Modulator: The cost here should include the cost of single photon transmission, detection and encoding using the conventional QSDC scheme, and it also includes photon transmission and detection costs when using the MDI-QSDC scheme. It should also be noted that we assume that the cost of encoding photons has been covered in the cost calculation of the light transmitter, which means that the photons emitted by the light transmitter are pre-coded photons.

Suppose that for a communication request r belonging to the request set R, the number of single transmissions of ciphertext between the source node s and the destination node d using MDI-QSDC scheme is n_m, and using conventional QSDC schemes is n_c. Each time the MDI-QSDC scheme is used, there are three uses of MDI-QSDC transmitters, one use of MDI-QSDC detector, and one use of conventional QSDC detector as described in Section II, while the conventional QSDC scheme process requires one use of conventional QSDC transmitter, one use of conventional QSDC detector, and one use of QSDC modulator. Let C_{MD}, C_{MT}, C_{CD}, C_{CT} and C_{CM} denote the cost of one use of MDI-QSDC detector, MDI-QSDC transmitter, conventional QSDC detector, conventional QSDC transmitter, and conventional QSDC modulator, respectively. Then the transmitter and receiver costs C_{TR} of communication request set R should be

$$C_{TR} = \sum_{r \in R} \frac{\mathfrak{C}_r}{\mathfrak{C}_S} \left[n_m \left(3C_{MT} + C_{MD} + C_{CD} \right) + n_c \left(C_{CT} + C_{CD} + C_{CM} \right) \right], \tag{1}$$

where $\mathfrak{C}_r$ is the communication capacity required for request r, $\mathfrak{C}_S$ is the capacity that the QSDC link can satisfy. Here, we use the secrecy capacity to represent the maximum secure communication rate that is achievable between two peer message nodes. In practice, the value of the secrecy capacity decreases as the distance between the communicating parties increases, and it is also influenced by various losses, noise, and the type of schemes used [33], [34]. For example, the multi-intensity QSDC scheme [26], which utilizes several intensities of weak laser pulses, has been investigated in a practical case of finite block lengths. When the transmission distance is $80\,\mathrm{km}$, a secrecy capacity of approximately 10^{-5} $\mathrm{bit/pulse}$ can be achieved by utilizing a specific implementation of the multi-intensity QSDC scheme over a fiber channel. For a more general consideration, the specific value of the secrecy capacity is not considered in this work, and we assume that the capacity between two adjacent nodes is the same for simplicity. We make this assumption relying on the actual network deployment. In actual networks, to ensure communication quality, repeaters need to be deployed between peer message nodes that are far apart. The maximum communication capacity between the peer message nodes is determined by the minimum communication capacity among those links connecting adjacent repeaters. To better integrate with the

classical networks, quantum networks are generally designed with a repeater deployed every $80\,\mathrm{km}$, which is similar to the deployment of erbium-doped fiber amplifiers in classical networks [22]. This means that the communication capacity between any two distant peer message nodes is maintained at the same level.

2) Cost of Security Facilities: In the QKD network based on trusted repeaters [22], the ciphertext will be converted into classical information at the repeaters. If a trusted repeater is attacked, information will be leaked. Therefore, additional costs are required to secure the trusted repeater. By contrast, in our QSDC network, untrusted-relay nodes acting as third-party measurement endpoints of the MDI-QSDC scheme will not gain information about the encrypted messages. Secure-relay nodes and peer message nodes will get the encrypted classical messages. These classical messages are encrypted by quantum-resistant algorithms. This avoids the cost of security facilities.

3) Cost of MU/DMU and Optical Switch Components: In order to more effectively transmit the photons and the classical header, we should deploy multiplexing devices in each repeater. Besides, the optical switch ensures that photons can be effectively transmitted to the correct path. It should be installed at each repeater, including peer message nodes, secure-relay nodes, and untrusted-relay nodes. Assume that the number of nodes that need to be passed between the source node s and the destination node d is n_t, and let C_m denote the cost of the use of a set of MU/DMU and optical switch components. Then, the cost C_M of the components of the communication request set R should be

$$C_M = \sum_{r \in R} C_m n_t. \tag{2}$$

4) Cost of QSDC Link: The link cost should consider the cost of using the conventional QSDC scheme and the MDI-QSDC scheme respectively.

For the conventional QSDC scheme, whether using the DL04 scheme or the QMF-QSDC scheme, the quantum channel should be used twice during the communication process. In detail, for the DL04 scheme [20], the message receiver should first use a conventional QSDC transmitter to send random photons to the message sender. The message sender encodes the photons and then transmits the photons through the quantum channel to the message receiver for measurement. For QMF-QSDC [25], although it has only experienced one photon transmission, in order for the subsequent communication, the random photons of the next round of transmission need to be transmitted to the other party in advance. Therefore, in terms of the number of times the channel is used, it is equivalent to using the quantum channel twice. Note that in conventional QSDC, we generally consider the photons and classical information of the security check to be a very small amount. In the cost simulation of this paper, we ignore this part of the cost.

For the MDI-QSDC scheme, the situation is different. When both ends of the peer message nodes or secure-relay nodes send photons to an untrusted-relay node for the first measurement, both photons need to pass through the quantum channel once. Then, the message sender transmits the second round of photons through the quantum channel. In the whole process, a total of three quantum channels need to be used. Likewise, we still ignore the cost of a small number of photons used for security checks.

It is assumed that the cost of different wavelength channels in a single fiber is the same. Let C_f denote the cost of using a single optical fiber for information transmission, l_c, l_m are the transmission distances using conventional QSDC and MDI-QSDC schemes respectively. Then the link cost C_L of communication request set R should be

$$C_L = \sum_{r \in R} \frac{\mathfrak{C}_r}{\mathfrak{C}_S} \left[3 l_m C_f / 2 + 2 l_c C_f\right]. \tag{3}$$

Note that the 2 in the denominator comes from the assumption that the transmission distance using the MDI-QSDC scheme is twice that of the conventional QSDC scheme. In fact, due to the efficiency of the detector, although the MDI-QSDC scheme will extend the communication distance, it is difficult to achieve twice the conventional QSDC scheme. However, in practice, we could assume that a repeater is deployed every $\zeta = 80\,\mathrm{km}$ for communication efficiency, and the secure transmission distance of the MDI-QSDC scheme is greater than $160\,\mathrm{km}$ [11]. Therefore, the distance assumption here is reasonable. In summary, the total usage cost C_{Total} of the hybrid QSDC network with secure-relay nodes and untrusted-relay nodes can be expressed as

$$C_{Total} = C_{TR} + C_{SF} + C_M + C_L. \tag{4}$$

In addition to some of the usage costs mentioned above, there are also some lower-cost optical auxiliary components and links that need to be set up when deploying the network. In this paper, we consider them to be inexpensive and ignore the cost of their use.

We have incorporated losses and non-idealities, such as detector inefficiency and detection error, into the point-to-point channel's secrecy capacity, acknowledging that these factors contribute to the non-ideal secrecy capacity. Furthermore, mitigating the impact of losses and non-idealities necessitates incurring higher equipment deployment costs. For instance, employing detectors with heightened detection efficiency would result in an augmentation of both C_{MD} and C_{CD}.

In a practical implementation, the synchronization of packet headers and quantum payloads is crucial for our two strategies. Nevertheless, in the current technological context, this problem can be mitigated within the SRN. At each node in the SRN, the ciphertext is read, re-encoded onto the quantum states, and routed to the next node. Hence, we can adopt a similar approach to deal with this problem, that is, to decode the quantum payload into classical information through a secure repeater. The decoded classical information can then be processed synchronously with the classical packet header to complete the forwarding of the quantum payload, while the decoded classical information will be encoded into the quantum payload. Under the structure we have designed, the

TABLE I
RELATIVE USAGE COST VALUES

QSDC Network	C_{MD}	C_{MT}	C_{CD}	C_{CT}	C_{CM}	C_{sf}	C_m	C_f
Relative cost (units)	2250	1500	2250	1500	1500	150	300	1

loss and decoherence of quantum states primarily occur during channel transmission, affecting costs by decreasing channel capacity. Hence, when quantum packet switching and quantum circuit switching strategies are used in the SRN, which serves as a key intermediate process for realizing the future full quantum network, there is no cost difference in the application of quantum state storage between the two strategies.

Furthermore, the ultimate quantum networks [35] will be built with a sufficient number of quantum devices. For instance, quantum memories [36] enable a more extensive application of quantum networks [37], where the quantum payload can be stored. For such devices, the effects of photon loss and decoherence on fidelity must be taken into account in such networks. Consequently, studying the cost of these devices, as well as their impact on the implementation of these two strategies, represents promising research directions.

B. Heuristic Cost Optimization Routing Algorithm

We propose a heuristic cost optimization routing algorithm (HCOA) to optimize the total cost of using a hybrid QSDC network with secure-relay nodes and untrusted-relay nodes. The specific algorithm is shown in Algorithm. 1. In our algorithm, it is assumed that the capacity resources of the classical control layer and the security check sublayer are sufficient.

In our algorithm, the *K-shortest-path* (KSP) algorithm is first used to find the route from the source node to the destination node and check whether the network resource meets the capacity need using the *First-Fit* algorithm. For all routes that meet capacity constraints, the cost is calculated based on the method provided in Section IV-A. Then, select the lowest-cost routing and update network status.

The total cost of deploying a QSDC network is highly dependent on technology updates and will also change with the development of processing levels within a certain period of time. Therefore, in this paper, we use the prices of existing commercial devices as well as consumables in Ref. [22], and use the relative prices of each device for discussion. The cost values used for evaluation and analysis are shown in Table. I. It should be noted that although experiments with small QSDC networks have been successful [7], no commercial QSDC device prices have yet been provided and some of the cost data are assumptions relying on those in Ref. [38]. Although this cannot best characterize the actual total cost of deployed devices, it is sufficient for our main discussion of the impact of deploying untrusted-relay nodes in the QSDC network and the effectiveness of the cost optimization algorithm, which can provide a certain reference for the deployment of QSDC network.

Algorithm 1 Heuristic Cost Optimization Algorithm

Data: Network topology graph G (node V, link E), request set $R = \{(s_r, d_r, \mathfrak{C}_r) : r = 1, 2 \ldots, n\}$ (request source node s_r, destination node d_r, requested capacity requirements $\mathfrak{C}_r$), cost parameters C_{MD}, C_{MT}, C_{CD}, C_{CT}, C_{sf}, C_m, C_f.

$C^R_{Total} = 0$;
foreach *communication request* $(s_r, d_r, \mathfrak{C}_r)$ *in set* R **do**
  Find routes $\mathcal{S}_r$ using *KSP* algorithm;
  $\mathcal{R}_r = \emptyset$;
  foreach P *in* $\mathcal{S}_r$ **do**
    if P *can be allocated the capacity resource using the First-Fit algorithm* **then**
      Append P to $\mathcal{R}_r$;
    end
  end
  if $\mathcal{R}_r \neq \emptyset$ **then**
    foreach P *in* $\mathcal{R}_r$ **do**
      Calculate n_m, n_c, n_t, n_s, l_m, l_s based on the route P;
      Calculate C_{TR}, C_{SF}, C_M, C_L according to the method we gave;
      $C^{r,P}_{Total} \leftarrow C_{TR} + C_{SF} + C_M + C_L$;
    end
    $C^r_{Total} \leftarrow \min_{P \in \mathcal{R}} C^{r,P}_{Total}$;
    $C^R_{Total} \leftarrow C^R_{Total} + C^r_{Total}$;
  else
    The request is blocked;
  end
  Update network status;
end

Result: C^R_{Total}, route and capacity allocated for the request, capacity utilization, blocking rate, etc.

When deploying the QSDC network, we can choose to deploy secure-relay nodes or untrusted-relay nodes according to the actual situation. In the following simulation, we assume two situations for discussion: the relay nodes set up in the network are all secure-relay nodes, and as many untrusted-relay nodes as possible are set up. It should be noted that both ends of an untrusted-relay node must be connected to a secure-relay node or a peer message node, which limits the maximum number of untrusted-relay nodes that can be assumed.

First, we discuss the cost parameter in two different situations. In order to better use mathematical formulas to represent

corresponding parameters, we first give the definitions of two functions that will be used in this paper.

- Round down function $f(x) = [x]$. It is defined as the largest integer strictly less than x.
- Binary function $g(x)$. It is defined as

$$g(x) = \begin{cases} 1, & \text{when } 2k\zeta < x \leq (2k+1)\zeta \\ 0, & \text{when } (2k-1)\zeta < x \leq 2k\zeta, \end{cases} \tag{5}$$

where $k \in \mathbb{Z}$. For the situation where secure-relay nodes are completely deployed between peer message nodes, the times of ciphertext transmission between the source node s and the destination node d using MDI-QSDC schemes n_m^c, and using conventional QSDC schemes n_c^c should satisfy

$$\begin{aligned} n_m^c &= 0, \\ n_c^c &= \sum_{(i,j)\in P_r} \left[\frac{l_{(i,j)}}{\zeta} + 1 \right], \end{aligned} \tag{6}$$

where (i,j) represents all the pairs of adjacent nodes on the route of request r passed from the source node to the target node. In this paper, for better communication effect, we set $\zeta = 80\,\mathrm{km}$. The number of secure-relay nodes n_s^c passed on the route and the number of all nodes n_t^c can be expressed as

$$\begin{aligned} n_s^c &= \sum_{(i,j)\in P_r} \left[\frac{l_{(i,j)}}{\zeta} \right], \\ n_t^c &= \sum_{(i,j)\in P_r} \left[\frac{l_{(i,j)}}{\zeta} \right] + k^c, \end{aligned} \tag{7}$$

where k^c is the number of peer message nodes experienced in routing from the source node to the destination node, and it is related to the selection of specific routes. The length of the optical fiber link transmitted using conventional QSDC schemes should be equal to the link distance between the source node and the destination node.

When we deploy as many untrusted-relay nodes as possible, we deploy an untrusted-relay node every $160\,\mathrm{km}$. If the distance between the last parts of two peer message nodes is less than ζ, we need to use the conventional QSDC scheme once to implement information transmission. For example, when the distance between two peer message nodes is $192\,\mathrm{km}$, we will deploy an untrusted-relay node and a secure-relay node between the two nodes. When information is transmitted between two nodes, an MDI-QSDC scheme is first used to transmit the information $160\,\mathrm{km}$ to the secure-relay node, and then a conventional QSDC scheme is used to complete the transfer of the information between the two peer message nodes. At this time, the times of transmission between the source node s and the destination node d through MDI-QSDC schemes n_m^m and using conventional QSDC schemes n_c^m should satisfy

$$\begin{aligned} n_m^m &= \sum_{(i,j)\in P_r} \left[\frac{l_{(i,j)} + \zeta}{2\zeta} \right], \\ n_c^m &= \sum_{(i,j)\in P_r} g\left(l_{(i,j)}\right). \end{aligned} \tag{8}$$

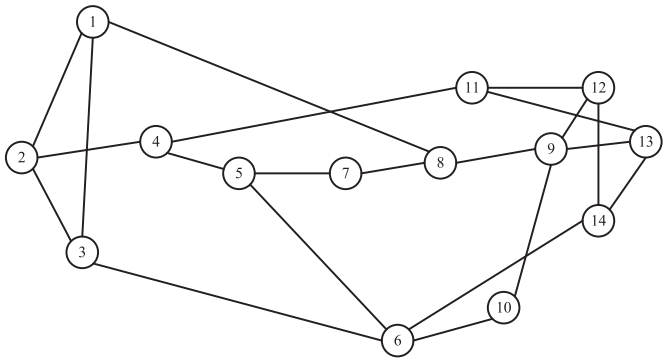

Fig. 5. The 14-node NSFNET network with 21 links.

The number of secure-relay nodes n_s^m passed on the route and the number of all nodes n_t^m can be expressed as

$$\begin{aligned} n_s^m &= \sum_{(i,j)\in P_r} \left[\frac{l_{(i,j)}}{2\zeta} \right], \\ n_t^m &= \sum_{(i,j)\in P_r} \left[\frac{l_{(i,j)}}{\zeta} \right] + k^c. \end{aligned} \tag{9}$$

When we deploy as many untrusted relay nodes as possible, we need to separately calculate the physical length of the optical fiber that transmits information through different schemes. The physical lengths corresponding to the two methods are

$$\begin{aligned} l_m^m &= \sum_{(i,j)\in P_r} \left((1 - n_c^m)\, l_{(i,j)} + 2\zeta \left[\frac{l_{(i,j)}}{2\zeta} \right] n_c^m \right), \\ l_c^m &= \sum_{(i,j)\in P_r} \left(n_c^m \left(l_{(i,j)} - 2\zeta \left[\frac{l_{(i,j)}}{2\zeta} \right] \right) \right). \end{aligned} \tag{10}$$

V. Simulation

In this section, we simulate the network with different configurations. All simulations are performed on the 14-node NSFNET network with 21 links as shown in Fig. 5. The specific parameters of the network are given in [39] and [40].

We refer to the behavior that a node tries to send a packet to another node as a request. In the packet switching strategy, the request is a transmission request. In the circuit switching strategy, the request is either a connection-establishment request or a packet delivery that uses an old connection. Here, the old connection means that there is at least one packet has been delivered in this connection. The capacity requirement of a request is the one that the packet delivery requires in the corresponding strategy. Requests between different nodes are randomly generated, and the capacity of a request is randomly generated from the set $\{0.04\mathfrak{C}_S, 0.08\mathfrak{C}_S, 0.12\mathfrak{C}_S, 0.16\mathfrak{C}_S, 0.2\mathfrak{C}_S\}$.

For simplicity, we consider the case that the SDN directly controls all routing. As connection is an important property of the quantum circuit switching strategy, the simulation will take a dynamic model into account. There are two types of phases in a simulation. The duration of one phase is short while the other is relatively longer. When the system is in the short one, which we call the processing phase, the nodes in the quantum

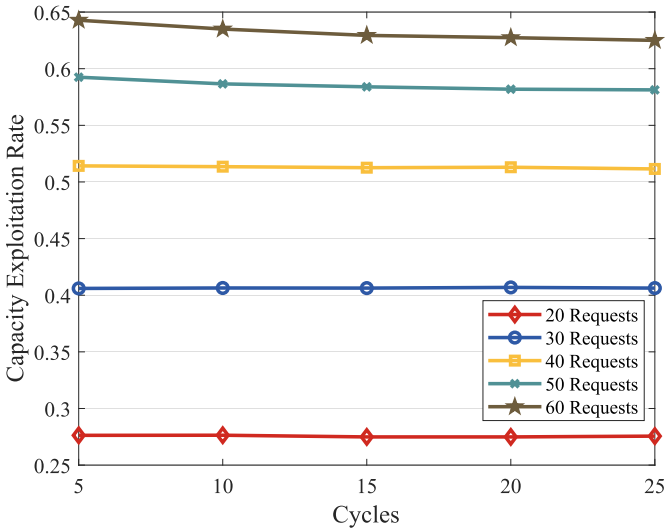

Fig. 6. Simulation results. Diagram of the relationship between the Capacity Exploitation Rate and the cycles. Different curves represent different numbers of requests generated in one cycle.

network send messages to the SDN according to the strategies that the nodes are using. Then the SDN decides a route if the request of the source node is accepted. Otherwise, it denies the request instead of sending the routing information to the nodes in the quantum network. In our simulation, we suppose that the SDN prioritizes the requests of the quantum circuit switching strategy. During the long phase, which we call the communication phase, the nodes in the quantum network send and forward the packets to communicate. In the quantum circuit switching strategy, a packet delivery may use an old connection. We still assume there is a processing phase before the packet delivery even if the source node doesn't need to ask the SDN for connection establishment in the processing phase.

We regard a processing phase and the subsequent communication phase as a unit in the simulation, which we call a cycle. A simulation consists of many cycles. The requests in one cycle can be divided into three types: the requests using old connections, the requests using new connections, and the requests using the quantum packet switching strategy. We call the latter two the new requests. If there is a connection that hasn't been closed in the previous cycle, a packet delivery in the connection can happen between the two nodes connected by the connection, which we call a request using an old connection. There may be some requests needing new connections to deliver in a cycle, which we call the requests using new connections. The left requests are those using the quantum circuit switching strategy. The duration of a connection is randomly selected to be 1-5 cycles. Obviously, when there are a large number of network requests in a cycle, some requests may be denied. The denied requests will enter the queue, and resources will be prioritized to them when the next cycle arrives.

The performance of the quantum network is assessed by three metrics, cost, blocking rate and capacity exploitation rate. We first give their definition in one cycle and then give their definition of a simulation. A cycle begins with random requests sent by nodes. The blocking rate is the percentage of requests that are denied in the cycle and is defined as follows:

$$[\text{Block Rate}] = \frac{[\text{The Number of Denied Requests}]}{[\text{ The Number of New Requests }]}. \quad (11)$$

The total cost of a cycle is not enough to characterize the state when the number of all requests is fixed, since additional requests do not change the cost if they are denied. Therefore, we introduce the efficient cost, which is

$$[\text{Efficient Cost}] = \frac{[\text{Cost}]}{(1-P)+P(1-[\text{Blocking Rate}])}, \quad (12)$$

where

$$P = \frac{[\text{Then Number of New Requests}]}{[\text{The Number of All Requests}]}. \quad (13)$$

The last metric is the capacity exploitation rate, which is

$$[\text{Capacity Exploitation Rate}] = \frac{\sum_{[\text{Link}]} [\text{The Used Capacity}]_{[\text{Link}]}}{\sum_{[\text{Link}]} [\text{The Capacity}]_{[\text{Link}]}}. \quad (14)$$

The summation goes over the links in the quantum network and a link is labeled by [Link]. $[\text{The Used Capacity}]_{[\text{Link}]}$ is the used capacity of the link labeled by [Link] and $[\text{The Capacity}]_{[\text{Link}]}$ is the capacity of the link labeled by [Link].

All definitions given above are within a cycle. The three metrics above can be extended to evaluate the performance of the quantum network of one cycle or multiple cycles, that is, a simulation. Here, we calculate them for every cycle in a simulation. The efficient cost of every cycle is the cost of a cycle divided by the proportion of unblocked requests in the cycle. The blocking rate is the percentage of denied requests out of the new requests, which consists of the requests using new connections and the requests using the packet switching strategy in the cycle. The capacity exploitation rate is based on the used capacity to transmit packages in the cycle. For a simulation, the total efficient cost is the sum of all cycles' efficient costs. The blocking rate and the capacity exploitation rate are averaged over all cycles.

We find the simulation result has been stable when there are 20 cycles for different numbers of requests, as shown in Fig. 6. Therefore, we set the simulation duration to 20 cycles in subsequent simulations. At the same time, in order to explore generality, we performed 5000 times of each simulation and took the average as the results we present.

A. Quantum Network Strategies

Here, we discuss the impact of choosing different strategies for communication on network performance.

We first consider a network in which all strategies used to communicate are the same. This means that all requests generated either use the quantum circuit switching strategy or all use the quantum packet switching strategy. The difference in the total effective cost as well as the blocking rate for different numbers of requests of a cycle is shown in Fig. 7. We can see that they will have higher total effective costs if the nodes construct a stable connection by using the quantum

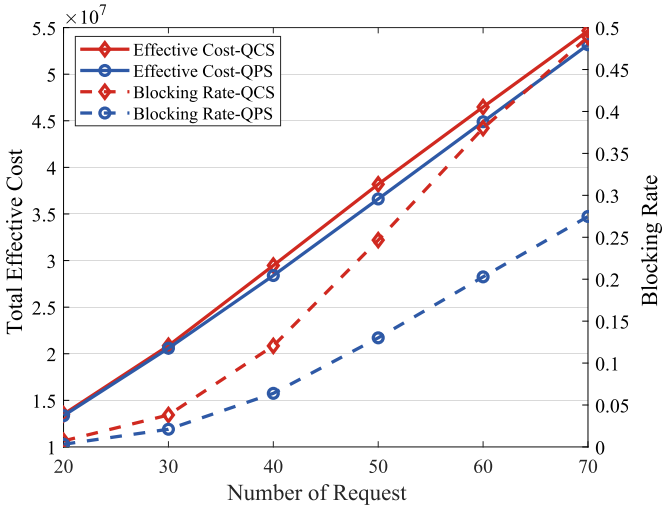

Fig. 7. Simulation results. Diagram of the relationship between the Total Effective Cost and the Number of Requests when all requests adopt quantum circuit switching (QCS) or quantum packet switching (QPS) strategy.

circuit switching strategy. At the same time, the higher blocking rate implies that the request is easier to deny when all nodes use the quantum circuit switching strategy. This is because the connection established in advance cannot be used by other requests in subsequent cycles, while requests using the quantum packet switching strategy can always use the optimal resource of the current network through the route optimization algorithm. Therefore, the quantum packet switching strategy has advantages in terms of the total effective cost and blocking rate. By contrast, the quantum circuit switching strategy can provide stable connections, which is more suitable for applications that do not have high-speed requirements but have high data integrity requirements, such as file transfer in wide-area networks. Meanwhile, the SDN tends to deny the request when the number of requests increases. The phenomenon is consistent for the quantum circuit switching strategy and the quantum packet switching strategy.

The application of two strategies at the same time is also considered. This means that some of the randomly generated requests choose the quantum packet switching strategy, and some choose the other one. Fig. 8a gives the blocking rate where half of the requests choose the quantum circuit switching strategy. As the requests of the quantum circuit switching strategy are prior to those of the quantum packet switching strategy for the SDN, the requests of the quantum circuit switching strategy share better resources of the quantum network and hence have a lower blocking rate even if the number of requests varies.

A more general result is shown in Fig. 8b. The blocking rate of the quantum circuit switching strategy is still lower at different percentage requests of the quantum circuit switching strategy. However, it should be noted that although the blocking rates of both strategies increase with the increase of the quantum circuit switching strategy percentage, the total blocking rate does not always increase. This is due to the change in the proportion of the two strategies causing the total blocking rate to eventually move closer to the blocking rate of the quantum circuit switching strategy. It can also be seen from Fig. 8b that if a small number of requests choose to use the other strategy instead in a network where all requests use the same strategy, the request blocking rate will increase. This implies that the network situation has become worse. It can also be reflected in the network resource exploration rate as shown in Fig 8c. However, the total effective cost becomes lower. For example, compared to using the quantum circuit switching strategy or quantum packet switching strategy, the total effective cost decreases by 0.93% and 4.18%, respectively, when the percentage of the quantum circuit switching strategy is 0.4. This means that network operators need to make a trade-off between network conditions and network costs.

Due to the inability to maintain connectivity, critical resources in a quantum network can easily be consumed by a small number of other requests, leading to an increase in the cost of transmitting packets using quantum packet switching strategies. In other words, the scarcity of quantum resources poses a challenge for quantum packet switching strategies to fully utilize quantum resources at a low cost. However, our simulation indicates that the quantum packet switching strategy can conserve more quantum resources than the quantum circuit switching strategy in terms of cost.

It should be noted that, for simplicity, we have assumed that the capacity between two adjacent nodes is the same in Sec. IV-A. Adjusting this assumption does not alter the conclusions regarding the network strategies. Changing the capacities between peer message nodes may lead to the selection of a different route compared to the existing one. Since both of our two network strategies use the same routing algorithm, the new routes chosen by both strategies will be identical. Hence, this change will not differentially impact the two network strategies. Additionally, by considering the trade-off between cost and capacity when deploying a network, it becomes feasible to optimize the total cost in a more realistic scenario, allowing for potential performance enhancements in the future.

B. Hybrid Deployment

The methods and devices employed for implementing point-to-point QSDC are markedly distinct from those utilized in classical communication systems. This distinction is evident in the varying numbers and types of devices required in both MDI-QSDC and the conventional QSDC schemes, posing novel challenges for resource allocation and deployment within quantum networks.

To show how infrastructure deployment affects the QSDC network, we let the network strategy be fixed and we first suppose that the network uses the quantum packet switching strategy to communicate. There are two ways to construct the network. We use total secure-repeater (TSR) to represent the network that is composed of total secure-relay nodes. The one in which the untrusted-relay nodes are deployed as many as possible is represented by partially secure-repeater (PSR).

The cost saved by the HCOA algorithm can be shown by comparing it with the random path algorithm (RPA). The RPA refers to first using the *KSP* algorithm to find the route from the source node to the destination node, and checking

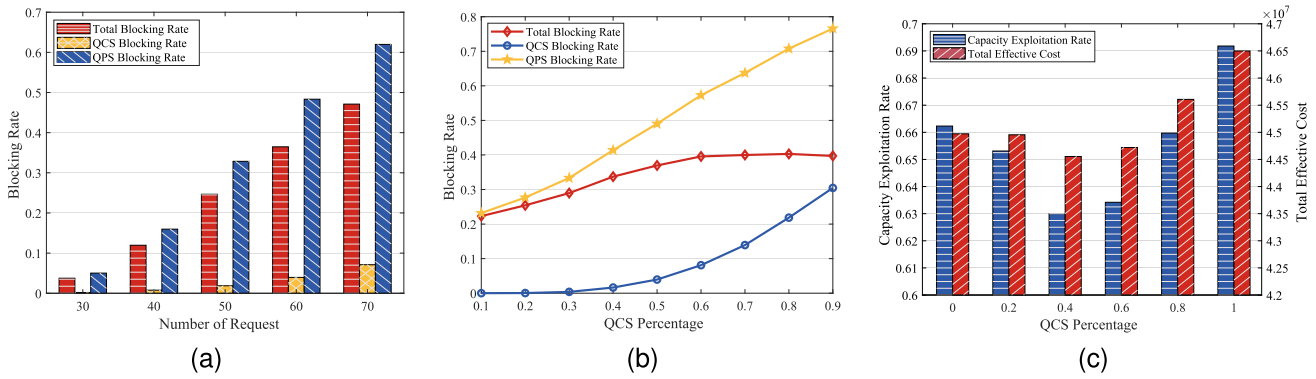

Fig. 8. Simulation Results. (a) Diagram of the relationship between the Blocking Rate and Number of Requests, when half of the requests use the quantum packet switching strategy and the other half use the quantum circuit switching strategy. (b) Diagram of the relationship between the Blocking Rate and the percentage of the requests using the quantum circuit switching strategy when the Number of Requests is 60. (c) Diagram of the Capacity Exploitation Rate and Total Efficient Cost at different percentages of the requests using the quantum circuit switching strategy when the Number of Requests is 60.

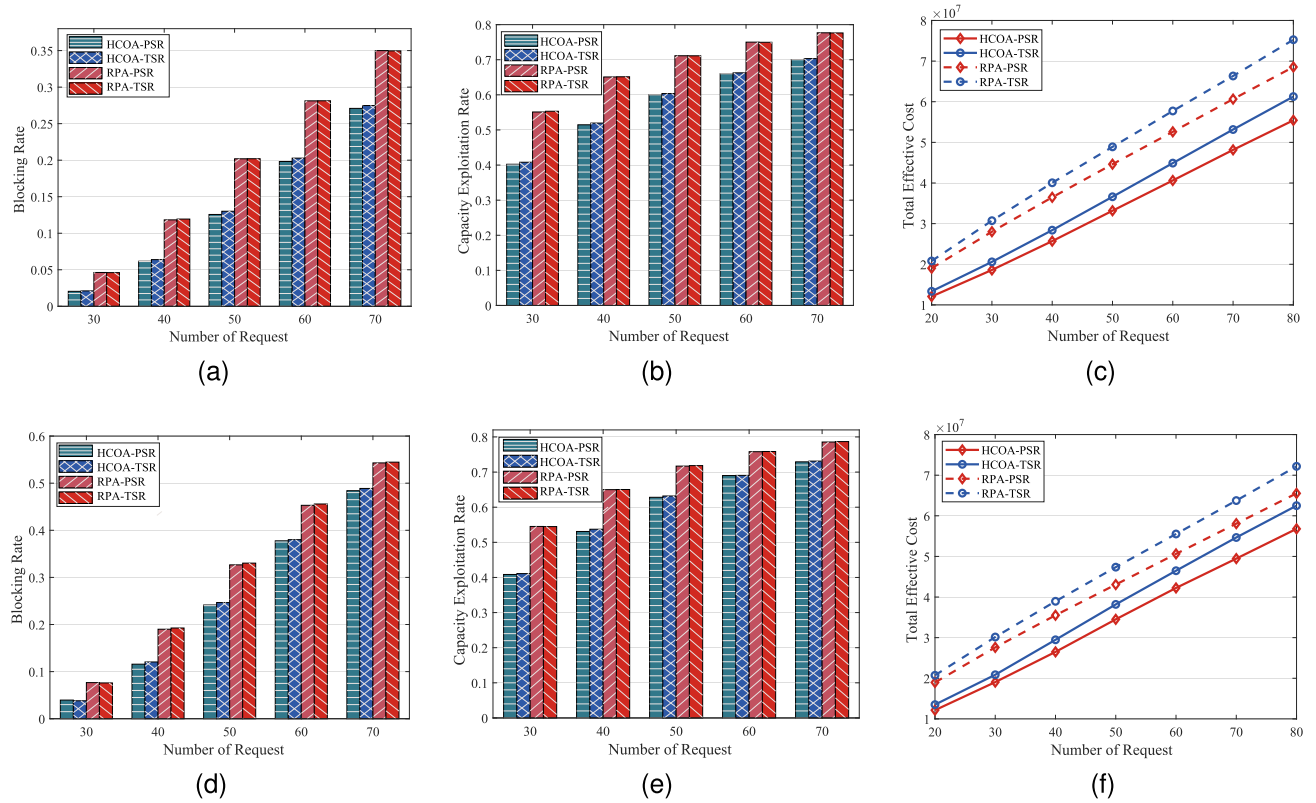

Fig. 9. Simulation Results. (a) Diagram of the relationship between the Blocking Rate and the Number of Requests used by different algorithms in networks with different deployment methods in the quantum packet switching strategy. (b) Diagram of the relationship between the Capacity Exploitation Rate and the Number of Requests used by different algorithms in networks with different deployment methods in the quantum packet switching strategy. (c) Diagram of the relationship between the Total Efficient Cost and the Number of Requests used by different algorithms in networks with different deployment methods in the quantum packet switching strategy. (d) Diagram of the relationship between the Blocking Rate and the Number of Requests used by different algorithms in networks with different deployment methods in the quantum circuit switching strategy. (e) Diagram of the relationship between the Capacity Exploitation Rate and the Number of Requests used by different algorithms in networks with different deployment methods in the quantum circuit switching strategy. (f) Diagram of the relationship between the Total Efficient Cost and the Number of Requests used by different algorithms in networks with different deployment methods in the quantum circuit switching strategy.

whether the capacity resources meet the need and passing the packet along the corresponding route. Among all feasible routes that meet the capacity requirements, a route is randomly selected as the communication route. This selection method is also used in current networks [41], and we can use it to characterize the upper bound of the capacity exploitation rate.

It can be seen from Fig. 9a and Fig. 9b, that HCOA can significantly reduce network capacity exploitation rate and request blocking rate. When the number of requests is between 30-50, the blocking rate is reduced to nearly half of the original value. This is because HCOA prefers to use fewer resources to complete the transmission of information for each request r, which will make network resources more

efficiently utilized and allow the network to satisfy more requests. For two different repeater deployment situations, the capacity exploitation rates and request blocking rates are not much different. This is because although there will be a large difference in cost for different repeater deployment scenarios, the difference in routing selection is not significant.

Fig. 9c shows the total effective cost of two network deployment conditions. Compared with the RPA, the HCOA plays a good role in optimizing the use cost and reduces the cost to a great extent. For example, when the number of requests is 40, the usage costs are reduced by 29.1% and 29.6% in TSR and PSR networks, respectively. This means that our HCOA algorithm saves total effective cost compared to the RPA algorithm in both networks. Although the degree of cost optimization achieved by the two deployment methods of HCOA is similar, the specific costs associated with each method differ. Compared with the TSR network deployment method, the PSR network usage cost is lower, with the average total efficient cost reduced by about 9.5%.

With the quantum circuit switching strategy, the improvement brought by HCOA is still significant, as shown in Fig. 9d, Fig. 9e, and Fig. 9f. Compared with the TSR network deployment method, the average total efficient cost of the PSR network is reduced by about 9.4%. It should be noted that we assume that the cost per use is the same regardless of the times the device is used. However, in practical applications, the cost may indeed decrease with an increasing number of requests [22], which is left to our future work.

Overall, the improvement of network performance parameters by our HCOA algorithm is significant. In both cases of using quantum circuit switching and quantum packet switching, it can better utilize network resources to ensure the operation of the QSDC network.

VI. Conclusion

In this paper, we give a QSDC network implementation and architecture, as well as focus on the network node structure in the QSDC network layer. By Combining this network architecture, we propose two strategies for quantum network communication: a quantum packet switching strategy and a quantum circuit switching strategy. We found that the former exhibits superior performance within a network, specifically, it demonstrates lower costs and reduced blocking rates. They provide a reference for future QSDC network implementation.

In order to better highlight the practical application value of the QSDC network, we propose a hybrid QSDC network method and a cost model for deploying secure-relay nodes and untrusted-relay nodes on existing optical networks. Simulation results for the two strategies show that the total effective costs of using the untrusted-relay nodes can both be reduced by about 9.4%, compared to fully deploying a secure-relay node network. We also give a heuristic cost-optimization algorithm for calculating network costs. In practical applications, our algorithm is not only more efficient in terms of network resource exploitation and request blocking rate, but it can also optimize network usage costs, which promotes the realization and application of the QSDC network.

In future work, it is worth studying further QSDC network costs under more specific and newer technologies. More efficient routing algorithms for larger networks should also be studied. Establishing an experimental platform to demonstrate a quantum network with the different quantum switching strategies would also be beneficial in promoting the practical implementation of QSDC.

References

[1] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 3, Feb. 2002, Art. no. 032302.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 175–179.

[3] L.-C. Kwek et al., "Chip-based quantum key distribution," *AAPPS Bull.*, vol. 31, no. 1, p. 15, Jun. 2021.

[4] C. Wei, X. Cai, T. Wang, S. Qin, F. Gao, and Q. Wen, "Error tolerance bound in QKD-based quantum private query," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 517–527, Mar. 2020.

[5] M. Caleffi and A. S. Cacciapuoti, "Quantum switch for the quantum Internet: Noiseless communications through noisy channels," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 575–588, Mar. 2020.

[6] H. J. Kimble, "The quantum Internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, Jun. 2008.

[7] G.-L. Long, D. Pan, Y.-B. Sheng, Q. Xue, J. Lu, and L. Hanzo, "An evolutionary pathway for the quantum Internet relying on secure classical repeaters," *IEEE Netw.*, vol. 36, no. 3, pp. 82–88, May 2022.

[8] E. Dubrova, K. Ngo, J. Gärtner, and R. Wang, "Breaking a fifth-order masked implementation of CRYSTALS-kyber by copy-paste," in *Proc. 10th ACM Asia Public-Key Cryptography Workshop*, New York, NY, USA, Jul. 2023, pp. 10–20.

[9] Z. Zhou, Y. Sheng, P.-H. Niu, L. Yin, G. Long, and L. Hanzo, "Measurement-device-independent quantum secure direct communication," *Sci. China Phys., Mech. Astron.*, vol. 63, no. 3, Dec. 2019, Art. no. 230362.

[10] P.-H. Niu, J.-W. Wu, L.-G. Yin, and G.-L. Long, "Security analysis of measurement-device-independent quantum secure direct communication," *Quantum Inf. Process.*, vol. 19, no. 10, p. 356, Sep. 2020.

[11] Z.-Z. Sun, D. Pan, D. Ruan, and G.-L. Long, "One-sided measurement-device-independent practical quantum secure direct communication," *J. Lightw. Technol.*, vol. 41, no. 14, pp. 4680–4690, Jul. 15, 2023.

[12] G. M. Saridis et al., "Lightness: A function-virtualizable software defined data center network with all-optical circuit/packet switching," *J. Lightw. Technol.*, vol. 34, no. 7, pp. 1618–1627, Apr. 1, 2016.

[13] N. D. E. Jerger, L.-S. Peh, and M. H. Lipasti, "Circuit-switched coherence," in *Proc. 2nd ACM/IEEE Int. Symp. Netw.-Chip (nocs)*, Apr. 2008, pp. 193–202.

[14] M. J. O'Mahony, D. Simeonidou, D. K. Hunter, and A. Tzanakaki, "The application of optical packet switching in future communication networks," *IEEE Commun. Mag.*, vol. 39, no. 3, pp. 128–135, Mar. 2001.

[15] D. J. Blumenthal, P. R. Prucnal, and J. R. Sauer, "Photonic packet switches: Architectures and experimental implementations," *Proc. IEEE*, vol. 82, no. 11, pp. 1650–1667, Nov. 1994.

[16] P. Andreades, K. Clark, P. M. Watts, and G. Zervas, "Experimental demonstration of an ultra-low latency control plane for optical packet switching in data center networks," *Opt. Switching Netw.*, vol. 32, pp. 51–60, Apr. 2019.

[17] J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, "Quantum Internet protocol stack: A comprehensive survey," *Comput. Netw.*, vol. 213, Aug. 2022, Art. no. 109092.

[18] Z.-Z. Sun, Y.-B. Cheng, Y.-C. Liu, D. Ruan, D. Pan, and G.-L. Long, "Message-oriented entanglement distribution network," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 35317–35328, Nov. 2024.

[19] D. Chandra, A. S. Cacciapuoti, M. Caleffi, and L. Hanzo, "Direct quantum communications in the presence of realistic noisy entanglement," *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 469–484, Jan. 2022.

[20] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A, Gen. Phys.*, vol. 69, no. 5, May 2004, Art. no. 052319.

[21] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "Sdn security: A survey," in *Proc. IEEE SDN Future Netw. Services (SDN4FNS)*, Nov. 2013, pp. 1–7.

[22] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Cost-efficient quantum key distribution (QKD) over WDM networks," *J. Opt. Commun. Netw.*, vol. 11, no. 6, pp. 285–298, Jun. 2019.
[23] L.-Q. Chen, M.-N. Zhao, K.-L. Yu, T.-Y. Tu, Y.-L. Zhao, and Y.-C. Wang, "ADA-QKDN: A new quantum key distribution network routing scheme based on application demand adaptation," *Quantum Inf. Process.*, vol. 20, no. 9, p. 309, Sep. 2021.
[24] Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu, and J. Zhang, "Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)," *Opt. Exp.*, vol. 25, no. 22, pp. 26453–26467, Oct. 2017.
[25] Z. Sun et al., "Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5778–5792, Sep. 2020.
[26] Z.-Z. Sun, D. Pan, Y.-B. Cheng, Y.-C. Liu, D. Ruan, and G.-L. Long, "Multi-intensity quantum secure direct communication relying on finite block-length," *IEEE Trans. Commun.*, vol. 72, no. 8, pp. 4633–4647, Aug. 2024.
[27] B. Mukherjee, "WDM optical communication networks: Progress and challenges," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 10, pp. 1810–1824, Oct. 2000.
[28] S. J. Ben Yoo et al., "Quantum wrapper networking," *IEEE Commun. Mag.*, vol. 62, no. 3, pp. 76–81, Mar. 2024.
[29] F. Zaman, U. Khalid, T. Q. Duong, H. Shin, and M. Z. Win, "Quantum full-duplex communication," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 9, pp. 2966–2980, Sep. 2023.
[30] X. Sun, M. Sopek, Q. Wang, and P. Kulicki, "Towards quantum-secured permissioned blockchain: Signature, consensus, and logic," *Entropy*, vol. 21, no. 9, p. 887, Sep. 2019.
[31] J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach*. Hoboken, NJ, USA: Pearson, 2016.
[32] A. S. Cacciapuoti, J. Illiano, and M. Caleffi, "Quantum Internet addressing," *IEEE Netw.*, vol. 38, no. 1, pp. 104–111, Jan. 2024.
[33] D. Pan et al., "The evolution of quantum secure direct communication: On the road to the qinternet," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 3, pp. 1898–1949, 3rd Quart., 2024.
[34] Z.-Z. Sun, Y.-B. Cheng, D. Ruan, and D. Pan, "Single-photon measurement-device-independent quantum secure direct communication," *Opt. Commun.*, vol. 569, Oct. 2024, Art. no. 130745.
[35] S. Wehner, D. Elkouss, and R. Hanson, "Quantum Internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, p. 9288, Oct. 2018.
[36] R. König, U. Maurer, and R. Renner, "On the power of quantum memory," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2391–2401, Jul. 2005.
[37] M. He, R. Malaney, and J. Green, "Global entanglement distribution with multi-mode non-Gaussian operations," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 528–539, Mar. 2020.
[38] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 9, pp. 2701–2718, Sep. 2021.
[39] Y. Pointurier, M. Brandt-Pearce, S. Subramaniam, and B. Xu, "Cross-layer adaptive routing and wavelength assignment in all-optical networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 6, pp. 32–44, Aug. 2008.
[40] A. Betker et al., "Reference transport network scenarios," *MultiTeraNet Rep.*, vol. 2023, pp. 1–15, Jan. 2003.
[41] C. Le Quoc, P. Bellot, and A. Demaille, "Stochastic routing in large grid-shaped quantum networks," in *Proc. IEEE Int. Conf. Res., Innov. Vis. Future*, Mar. 2007, pp. 166–174.

Ze-Zhou Sun received the B.S. degree from Tianjin University, Tianjin, China, in 2021, where he is currently pursuing the Ph.D. degree. His current research interests include quantum communication and quantum networks.

Yuan-Bin Cheng received the B.S. degree from the Huazhong University of Science and Technology, Wuhan, China, in 2021. He is currently pursuing the Ph.D. degree at Tsinghua University, Beijing, China. His current research interests include quantum communication and quantum information theory.

Dong Ruan was born in 1970. He received the Ph.D. degree from Tsinghua University, Beijing, in 1997. He is currently a Professor with Tsinghua University. He is also the Deputy Chair of the Department of Physics, Tsinghua University; the Deputy Chair of the National College Steering Committee on Physics Major Teaching, MOE; and the Vice President of the Beijing Physical Society. His research interests include quantum computing, quantum physics, and mathematical physics.

Dong Pan (Member, IEEE) received the B.S. degree from Northwest University, Xi'an, China, in 2016, and the Ph.D. degree from Tsinghua University, Beijing, in 2021. From 2018 to 2019, he was a Visiting Student with the University of Southampton, Southampton, U.K. He is currently an Assistant Research Scientist with Beijing Academy of Quantum Information Sciences. His current research interests include quantum communication and quantum networks.

Fei-Hao Zhang received the B.S. degree from Shandong Normal University, Jinan, China, in 2012, and the Ph.D. degree from Tsinghua University, Beijing, China, in 2019. From 2013 to 2014, he was a Visiting Student with the University of Waterloo, Waterloo, Canada. He is currently an Assistant Research Scientist with Beijing Academy of Quantum Information Sciences. His current research interests include quantum communication and quantum networks.

Gui-Lu Long (Member, IEEE) received the B.S. degree from Shandong University in 1982 and the Ph.D. degree from Tsinghua University in 1987. Since then, he has been with Tsinghua University. From 1989 and 1993, he was a Research Fellow with the University of Sussex, U.K. He is currently a Professor with Tsinghua University. Notably among his various contributions, he proposed the theory of quantum secure direct communication in 2000, which is one of the three major quantum secure communication theories; constructed a quantum exact search algorithm, sometimes called Grover-Long algorithm; and established the linear combination unitaries (LCU) method, which is widely used in quantum algorithm designs. He has published more than 300 articles in refereed international journals. His research interests include quantum communication and computing and optical microcavity. He is a fellow of IoP, U.K.; and APS, USA. He served as the President of Associations for Asian Pacific Physical Societies (2017–2019) and the Vice-Chair for C13 of IUPAP (2015–2017).