Chapter

Multipoint-Interconnected Quantum Communication Networks

Qingcheng Zhu, Yazi Wang, Lu Lu, Yongli Zhao, Xiaosong Yu, Yuan Cao and Jie Zhang

Abstract

As quantum computers with sufficient computational power are becoming mature, the security of classical communication and cryptography may compromise, which is based on the mathematical complexity. Quantum communication technology is a promising solution to secure communication based on quantum mechanics. To meet the secure communication requirements of multiple users, multipoint-interconnected quantum communication networks are specified, including quantum key distribution networks and quantum teleportation networks. The enabling technologies for quantum communication are the important bases for multipoint-interconnected quantum communication networks. To achieve the better connection, resource utilization, and resilience of multipoint-interconnected quantum communication networks, the efficient network architecture and optimization methods are summarized, and open issues in quantum communication networks are discussed.

Keywords: multipoint-interconnected, quantum communication networks, quantum key distribution, quantum teleportation

1. Introduction

Quantum communication such as Quantum Key Distribution (QKD) and Quantum Teleportation (QT) is capable of exploiting the principles of quantum mechanics to transport classical, or even quantum, bits of information. quantum communication networks extend the concept of quantum communications, since they can transport, elaborate, and store quantum information (qubits) between different node pairs. Quantum communication networks leverage the principles of quantum mechanics including no-cloning, quantum measurement, entanglement, and teleporting. Hence, the new networking and computing capabilities emerge. At the same time, new and challenging constraints are imposed on the design and operations of quantum communication networks. This chapter firstly introduces the quantum communication enabling technologies including QKD and QT; then focuses on the research about QKD networks and QT networks to enable multipoint interconnection such as the architecture and service provisioning algorithms; finally, pays attention to problems and challenges of QT networking.

2. Quantum communication enabling technologies

The realizations of quantum communication network mainly include quantum key distribution technology and quantum teleportation technology.

2.1 Quantum key distribution

Quantum cryptography, which applies quantum properties to design the secure communication system, is the subset of quantum communication. QKD technology is a realization of quantum cryptography. It generates and distributes symmetrical cryptographic keys with information theoretical security based on the fundamental laws of quantum physics, i.e., the security is independent of all future advances of algorithm or computational power. QKD has the characteristic of "point-to-point" implementation. Thanks to the developments of quantum relay and switching technologies, the long-distance QKD is enabled. The following two subsections briefly introduce the QKD implementation and the related quantum relay and switching technologies to realize long-distance quantum communication.

2.1.1 Quantum key distribution implementation

The first quantum key distribution (QKD) protocol, the famous BB84 protocol, was proposed by Charles Bennett and Gilles Brassard in 1984 [1]. Since then, a series of QKD protocols such as E91, B92, SARG04, COW, DPS, GG02, MDI-QKD have been proposed one after another. There are three main implementation technologies of QKD: Discrete-Variable Quantum Key Distribution (DV-QKD), Continuous-Variable Quantum Key Distribution (CV-QKD), and Measurement Device-Independent Quantum Key Distribution (MDI-QKD). DV-QKD encodes information on a single photon and uses a single-photon detector for detection. DV-QKD originated earlier and is more mature, with a longer safe transmission distance. Besides, multi-node quantum network has been successfully established. The disadvantage is that single-photon sources are tricky to prepare [2]. Unlike DV or qubit-based QKD, the secret keys in CV-QKD are encoded in quadrature of the quantized electromagnetic field and decoded by coherent detections, which is lower cost and more practical. Under the same conditions, the output key rate of CV-QKD is much higher than that of the DV-QKD, and it is highly integrated with traditional optical communication networks. However, the current CV-QKD technology is not as good as the DV-QKD technology in terms of safe transmission distance, and the problem of working bandwidth also needs to be further resolved [3]. The security of MDI-QKD does not depend on whether the quantum device is trusted or not. MDI-QKD completely removes all security loopholes in the detection system and ensures a QKD network security with untrusted relays. Compared with CV-QKD, MDI-QKD can obtain higher security key rate, but the communication distance is shorter, and the channel is required to be asymmetric (that is, the measurement equipment is required to be close to the user on one side) [4].

In the past 10 years, a series of small-scale QKD technology verification networks have been built abroad, covering local area networks, metropolitan area networks, and intercity networks [5–9]. At the same time, a number of major technical research studies have been carried out in China to address quantum secure communication. Local area networks, metropolitan area networks, intercity networks, and wide area networks have carried out related work, including the quantum communication Beijing-Shanghai trunk line project for connecting metropolitan area networks, and the planned satellite-ground integrated wide-area

quantum communication network. To keep faint quantum signals apart from intensive classical data signals, traditional QKD networks utilize low-noise dedicated fibers, such as dark fibers, which will significantly increase QKD deployment cost. Also, researchers have studied how to combine QKD deployment onto existing optical networks [10].

2.1.2 Quantum relay and switching

There are two main ways to achieve long-distance QKD, namely quantum relay technology and quantum switching technology. On the one hand, quantum relay technology can solve the problem of exponential attenuation of photon signal transmission in optical fiber for long-distance QKD. There are currently two types of quantum relay technologies. One is based on trusted relay, and the other is based on quantum relay. The trusted relay scheme is to cache the key generated by the point-to-point link in the trusted relay node and then transmit the end-to-end key required by the user hop-by-hop through the multi-hop link using one-time pad. This scheme breaks through the transmission distance limitation of the QKD link, but the relay node for key transmission must be trusted [11]. The quantum relay scheme is to use the principle of quantum entanglement to realize the storage and forwarding of quantum states, so as to realize the long-distance distribution of quantum states [12]. In order to overcome the fading of quantum information during quantum channel transmission, using quantum nodes instead of optical nodes to transform quantum information can effectively increase the transmission distance. Quantum nodes with this function are usually called quantum repeaters. This technology does not require trustworthy relay nodes, but it is still in the stage of theoretical research. On the other hand, in quantum switching technology, trusted relay is mainly used by switching nodes of quantum secure communication network based on single core fiber. Through relay nodes, the "Beijing-Shanghai trunk line" passes through Beijing, Jinan, Hefei, and Shanghai, connecting Beijing and Shanghai's quantum key distribution metro-network, which can provide data transmission based on quantum encryption for government affairs, finance, and other fields [13]. In 2018, Travis S. Humble et al. designed and implemented software-defined quantum networking protocol and soft switch to support the integration of quantum communication and existing optical communication [14]. In 2020, by integrating the fiber and free-space QKD links, the QKD network in China has been extended to a total distance of 4600 km, where any user in the network is able to communicate with any other [9].

2.2 Quantum teleportation

QT involves the transportation of an unknown quantum state from one location to another, without physical transfer of the information carrier [15]. It is one of the main technologies for constructing quantum communication networks.

2.2.1 Quantum teleportation implementation

QT is a quantum information transmission method using the uncertainty of quantum entanglement to realize the remote transmission of quantum states, which is one of the main technologies for constructing quantum communication network [15]. In 1993, Bennett et al. first proposed a theoretical protocol based on Einstein-Podolsky-Rosen entangled photons for teleportation [16]. The main idea is that the communication parties share a pair of entangled particles to establish a quantum

channel, and the sender will transmit the unknown. After the quantum state and the shared particle perform a specific measurement on the local particle, the measurement result is notified to the receiving end, and the receiving end user performs a quantum gate operation on the particles owned based on the measurement result to obtain the quantum state to be transmitted by the sending end. It is worth noting that in the process of QT, the physical particles at the sender are not transmitted to the receiver but always stay in the sender. What is transmitted is only the quantum state, and the sender can even have nothing to do with this quantum state.

In 1997, the Zeilinger Research Group in Austria first reported the QT experiment in "Nature" [17]. The experimental results confirmed the feasibility of QT with a success rate of 25%. Since then, many scholars have developed theories of QT, exploring how to use different entangled states to construct quantum channels in the process of teleportation or how to transmit multi-qubit quantum states. In the current teleportation network experiment, the challenge is taken and a 30 km optical-fiber-based quantum network distributed over a 12.5 km area is constructed, which is robust against noise in real world with active stabilization strategies, allowing us to realize QT with all the ingredients simultaneously [18]. In Calgary fiber network, QT is reported from a telecom photon at 1532 nm wavelength, interacting with another telecom photon onto a photon at 795 nm wavelength. It improves the teleportation distance to 6.2 km [19].

2.2.2 Entanglement swapping and quantum repeaters

Quantum entanglement is a unique property of quantum systems, and it is also an important communication resource in QCNs. In principle, quantum entanglement is based on quantum superposition state [20]. Since quantum superposition experiments only reflect the indistinguishability of physical processes and are not limited to any specific physical quantities (such as momentum, energy, position, polarization, etc.), quantum entanglement is essentially not necessarily related to any specific physical quantities. The characteristics of quantum superposition have led many scholars to use a variety of methods to successfully prepare entangled states in experiments. For example, there are two typical methods for entangled photon generation technology based on parametric down conversion. The first type of entanglement source is the II-type phase-matched nonlinear crystal entanglement source [21]. The second entanglement source uses collinear nonlinear crystals to generate entanglement [22]. In addition, there is also the use of photonic crystal fibers to generate entangled photon pairs [23].

3. Quantum key distribution network

QKD generates and distributes symmetrical cryptographic keys with information theoretical security based on the fundamental laws of quantum physics, i.e., the security is independent of all future advances of algorithm or computational power. Quantum key distribution network (QKDN) is a network comprising two or more QKD nodes connected through QKD links, which allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

Although the international research on QKD is getting more and more in-depth, the research focus has always been on the performance improvement of the "point-to-point" QKD system, that is, how to increase the rate of quantum key generation, reduce the qubit error rate, and improve quantum key transmission distance, etc. It is difficult to use point-to-point QKD technology to support encryption requirements of various services from many nodes, and the security of services cannot be

guaranteed. Therefore, it is urgent to establish a QKDN that supports multipoint interconnection. This part will introduce the existed research about QKDNs, including the QKDN architecture, trusted repeater node structure, routing and resource allocation, key pool construction, resilience, and machine learning application.

3.1 The QKDN architecture

Optical networks today represent a fundamental infrastructure for data transport in the Internet, with more than 2 billion km of fiber deployed globally. To integrate QKD into existing optical networks, an architecture of QKD-enabled optical network with software-defined networking technology is proposed [24], as shown in **Figure 1**. It satisfies the needs of key resource pooling, network openness, and pipeline flexibility. The architecture consists of four planes: application (app) plane, control plane, QKD plane, and data plane, in top-down order.

The application plane generates connection requests. It is at the top of this architecture and is the destination of the final application of quantum keys. It uses the shared key pair provided by QKDN to perform encrypted communication between users. It mainly includes two application types: key application and network application.

The control plane is implemented using an SDN controller and is in charge of resource management and allocation for the QKD plane and data plane. The control plane is the core module of the QKDN architecture. It controls the key distribution behavior of the QKD plane through the south-bound interfaces between the control plane and the QKD plane and communicates with the application layer. Introducing SDN is beneficial for managing the entire network's resources via logically centralized control. The north-bound interfaces of control plane open up network capabilities to the application plane. At the same time, the control plane can control the key supply strategies and complete the information interaction. Specifically, functions in the control plane of QKDN include QKDN topology acquisition, network virtualization, QKDN path calculation and resource allocation, QKD application registration, QKD service configuration, link control, policy control, notification processing, and quality of service control. The control plane also supports connection control, network optimization, and the ability to provide third-party applications in multi-domain, multi-technology, multi-level, and multi-vendor QKDN. In order to realize the scalability of the control plane, the control plane should also support hierarchical structure, multiple control domain division, and controller hierarchical nesting, etc.

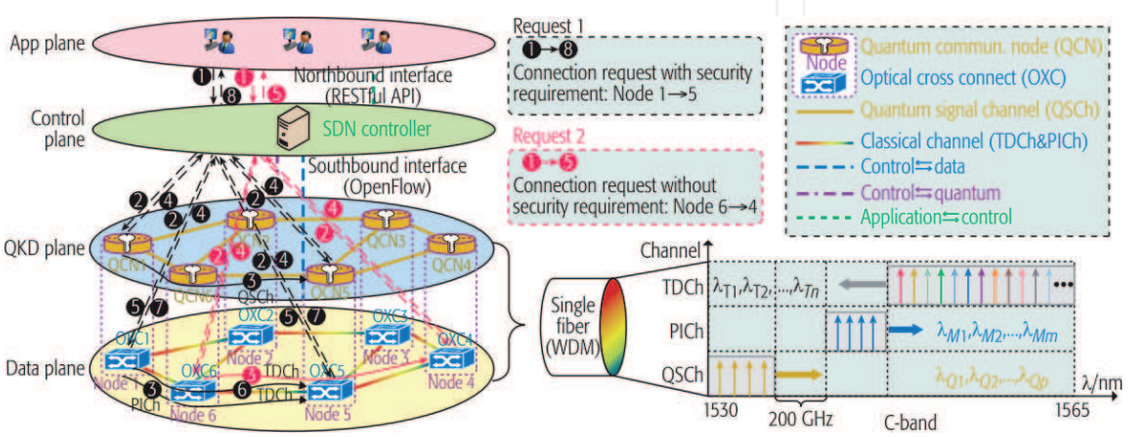

Figure 1.
The architecture of QKD-enabled optical network [24].

For each optical connection to be established in the network, in addition to the data channel (DCh), QKD requires a quantum channel (QCh) and a public channel (PCh) for secure key synchronization [25]. The QKD plane and data plane share fiber spectrum resources using WDM technology to construct QSCh, PICh, and TDCh. **Figure 1** shows a possible distribution of different channels in the fiber C-band. PICh and TDCh belong to the data plane. They can use general transmitters and receivers. Quantum communication node (QCN) has quantum switching functions: quantum signal sending and quantum signal receiving. It can use existing technologies for quantum switches, quantum transmitters, and quantum receivers [26]. Physically, an optical cross-connect (OXC) and a QCN are co-located at one node.

There are two types of connection requests in QKDNs including connection requests with and without security requirements. For example, when a connection request arrives with security requirements from node 1 to node 5 shown in **Figure 1** using black solid lines, SDN controller computes and allocates resources for channels including TDCh, PICh, and QSCh. In contrast, when the connection request arrives without security requirements from node 6 to node 4 shown in **Figure 1** using red solid lines, it is served by TDCh in data plane. The procedures of signals for configuring the two requests are delineated using black and red dashed lines in **Figure 1**, respectively. For the connection request with security requirement, the construction of QSCh and PICh for secure key synchronization is completed (steps 2–4), and the construction of TDCh is completed (steps 5–7).

3.2 Trusted repeater nodes structure

To overcome the distance limitation of QKD, either quantum repeaters or trust repeater nodes (TRNs) are required. However, the feasibility of quantum repeaters has yet to be demonstrated in practical long-distance QKD networks [27]. The TRN technique is a solution to construct long-distance QKD, and it has been widely adopted for the deployed QKD networks such as the deployed 2000 km QKD backbone network between Beijing and Shanghai in China recently.

An example of long-distance QKD based on TRNs is illustrated in **Figure 2** [28]. QBN_{src} and QBN_{dest} act as the source and destination QKD backbone nodes (QBNs) of two QKD users. TRN_1 and TRN_2 are deployed between QBN_{src} and QBN_{dest}. Three QKD links are separately established between QBN_{src} and TRN_1, TRN_1 and TRN_2, and TRN_2 and QBN_{dest}, while secret keys K_{s1}, K_{12}, and K_{2d} are separately produced on the three QKD links. To enable long-distance QKD between QBN_{src} and QBN_{dest}, four steps are performed as follows.

1. TRN_1 uses secret key K_{12} to encrypt secret key Ks1 and obtains the encrypted message $K_{12} \oplus K_{s1}$.

2. TRN_1 sends the encrypted message $K_{12} \oplus K_{s1}$ to TRN_2. TRN_2 uses secret key K_{12} to decrypt $K_{12} \oplus K_{s1}$ and obtains secret key K_{s1}.

3. TRN_2 uses secret key K_{2d} to encrypt secret key K_{s1} and obtains the encrypted message $K_{2d} \oplus K_{s1}$.

4. TRN_2 sends the encrypted message $K_{2d} \oplus K_{s1}$ to QBN_{dest}. QBN_{dest} uses secret key K_{2d} to decrypt $K_{2d} \oplus K_{s1}$ and obtains secret key K_{s1}.

Finally, QBN_{src} and QBN_{dest} can share the secret key K_{s1}. To guarantee the ITS of secret keys, one-time pad cryptosystem is required to be used for encryption. To

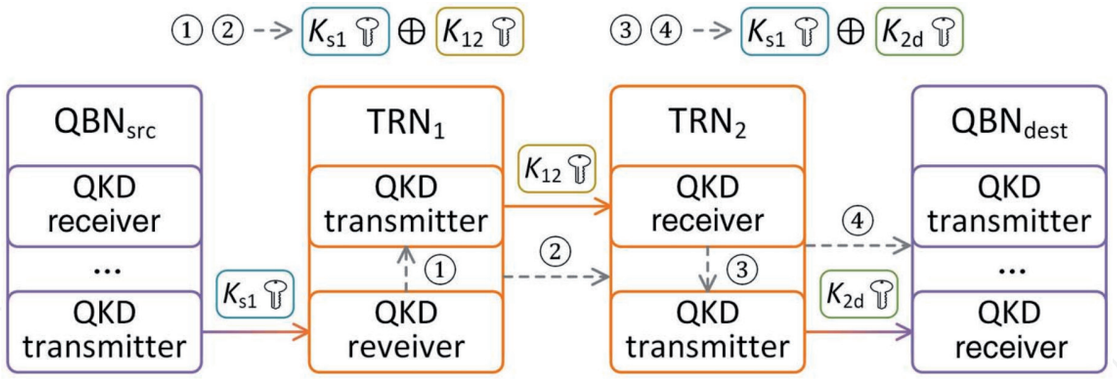

Figure 2.
Example of long-distance QKD based on TRNs [28].

extend the distance of QKD, a number of TRNs can be applied. Note that, each TRN is required to be trustworthy.

3.3 Routing and resource allocation in QKDN

With the expansion of the network scale, the number of users, and the continuous increase of security services, the problems of insecure key distribution process and low resource utilization in the key scheduling process in the prior art have become more and more prominent. To accomplish the key supply for services in QKDN effectively, the QKDN needs an efficient routing and resource allocation algorithm.

To accomplish the key supply for services, the concept of key as a service (KaaS) is proposed in [29]. Its meaning is providing secret keys as a service in a timely and accurate manner to satisfy the security requirements. The typical functions of KaaS are secret-key deployment and employment. To enable these functions, two secret-key virtualization steps are proposed including key pool (KP) assembly and virtual key pool (VKP) for secret-key deployment. For the KP assembly, the secret keys stored in each pair of key storages can be virtualized into a KP to facilitate secret-key resource management (e.g., KPA-B between KS-A and KS-B). For VKP assembly, a portion of secret keys in a KP can be virtualized into a VKP to enhance the security of dedicated service transmission (e.g., $VKP_{A\text{-}B\text{-}1}$ or $VKP_{A\text{-}B\text{-}2}$ abstracted from $KP_{A\text{-}B}$). Hence, with the combined two steps, the secret keys can be deployed and employed for securing different services in QKDNs.

Given that only finite wavelength resources can be reserved as QKD links, the time-scheduled technique can be applied to increase efficiency by dividing each wavelength channel for QCh/PCh into multiple time slots. Then, through the sharing of QCNs and QKD links in different time slots, the assembly of KPs can be realized between node pairs. The granularity of a time slot, which is denoted by t, is the synchronization time to produce a fixed number N of secret keys after KP assembly between two directly interconnected nodes. Note that, the synchronization time includes the time for channel estimation and calibration, qubit exchange, key sifting, and key distillation. Considering the constant consumption of the secret keys in KPs by the services for encrypting and decrypting data, the periodical KP assembly is needed to compensate for secret-key consumption. The period of KP assembly is denoted by T. Note that $t < T$, which ensures that KP assembly can be realized within a period.

As shown in **Figure 3**, a static time-shared KP assembly strategy for efficient secret-key deployment based on the Dijkstra and first fit (FF) algorithms is

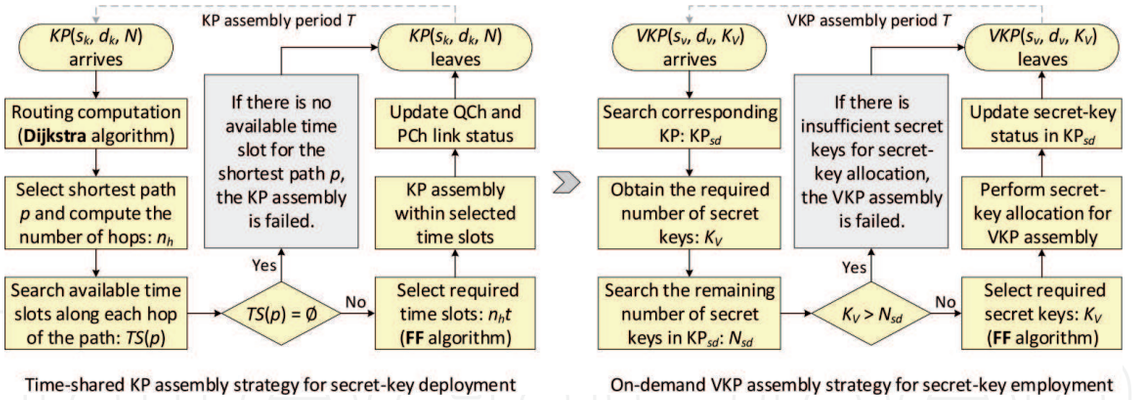

Figure 3.
KP and VKP assembly strategies for key supply [29].

presented. The KP assembly request is denoted by $KP(s_k, d_k, N)$, where s_k and d_k denote the source and destination nodes of the KP assembly request. The number of KPs is calculated by $n(n-1)/2$ since that KP is assembled between any pair of nodes. Here, n is the number of nodes in a QKDN. To compute and select the shortest QKD path between two nodes efficiently, the Dijkstra algorithm is utilized. The number n_h of hops is also computed, which aims to determine the required number of time slots. Then, to allocate available time slots for the assembly of different KPs, the FF algorithm is utilized.

After KP assembly, secret-key resource becomes a novel resource dimension in QKDNs, which can be virtualized. The virtualized KP is denoted as VKP. By assembling VKPs, the confidential services can be secured. Considering the different security requirements of services, different VKPs can require different numbers of secret keys. The type of VKPs with different secret-key resource requirements is denoted by V. The VKP assembly for secret-key employment is needed to satisfy the specific secret-key requirement of each VKP. The required secret keys for the assembly of a VKP are denoted by K_V. Secret keys will be updated and reallocated for VKP assembly when the KPs are assembled again. The updating and reallocating secret keys are necessary to enhance the security of confidential services.

Figure 3 presents a static on-demand VKP assembly strategy for efficient secret-key employment. The VKP assembly request is denoted by $VKP(s_v, d_v, K_V)$, where s_v and d_v are the source and destination nodes of the VKP assembly request. Secret-key resources cannot be reutilized, which are different from conventional computing, switching, and wavelength resources. Accordingly, some complicated resource allocation algorithms in conventional network scenarios such as most-used and load-balanced algorithms are not suitable for allocating secret keys in QKDNs. But the FF algorithm, which has high feasibility, can be utilized to allocate secret keys for the VKP assembly. The secret-key resources can be efficiently utilized and allocated using the on-demand VKP assembly strategy.

The simulations show the benefits of KaaS for efficiently deploying and employing secret keys as well as for security enhancement, where the balance of KPs' secret-key resources and VKPs' secret-key requirements can be achieved.

3.4 Key pool construction in QKDN

Aiming at the problem of low utilization of key resources in QKDNs, and the need to balance the inflow and outflow of key resources, a construction mechanism of virtual quantum key pools (QKPs) in QKDN is proposed [30], which achieves reasonable scheduling and efficient use of channel resources and key resources.

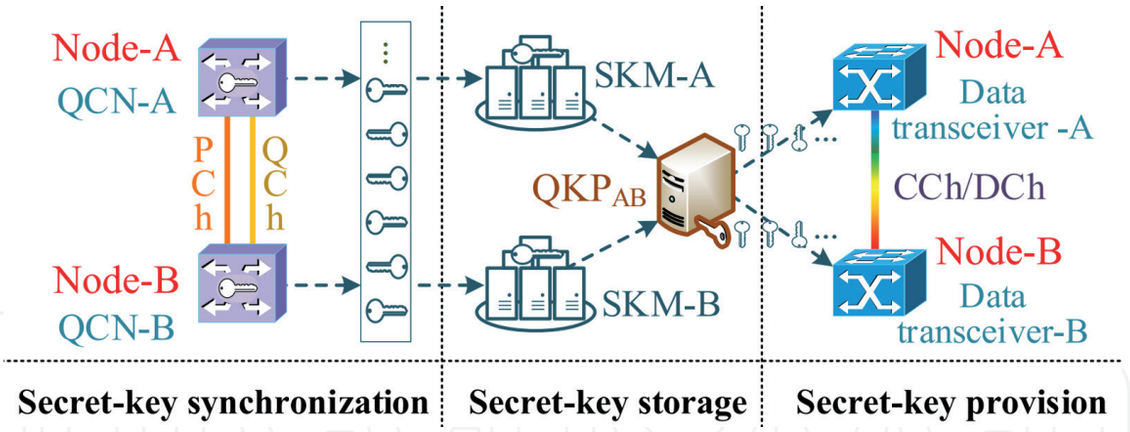

Figure 4.
QKP in point-to-point QKD system [30].

The extension of QKD from point-to-point systems to network-wide multipoint-interconnected systems requires to enhance the secret-key synchronization, storage, and provision, which improves the resource management and security performance. QKP construction in QKDNs is a potential solution to satisfy these requirements. In each node, there is a secret-key memory (SKM), which stores the synchronized secret keys. To improve the secret-key management, secret keys between each pair of SKMs are virtualized into a QKP, which is also denoted as VKP. QKP between the two nodes dynamically provides different numbers of secret keys for encrypting data according to different security requirements. **Figure 4** shows an example of QKP in point-to-point QKD system including QKD enhancements in secret-key synchronization, storage, and provision.

There are three main steps for constructing QKPs [30]:

- QCN-A encodes and transmits quantum signals to QCN-B via QCh.
- QCN-A and QCN-B interchange public information via PCh, so as to accomplish secret-key synchronization.
- After synchronization, SKM-A and SKM-B store secret keys between QCN-A and QCN-B respectively. The secret keys between SKM-A and SKM-B are virtualized to construct QKP_{AB}, which enables key supply on demand between Node-A and Node-B according to different security requirements through the CCh or DCh.

As for the support techniques for QKPs, QKPs are constructed on the control plane to manage the secret keys between QKD node pairs. They are all controlled by the SDN controller and can manage secret-key exchange, storage, assignment, and destruction. The SDN controller with programmable and flexible network control capabilities can also provide the effective implementation technique for QKPs.

4. Resilience of QKDN

The occurrence of failure is inevitable in QKDNs. Resilience of QKDN is very important. The key distribution on the corresponding routes will be disrupted, and key provisioning services will be affected by the failure of a single link. The security demands of users are intuitively violated. Apart from that, a high recovery time and capital expenditure will be indirectly induced further by such interruption.

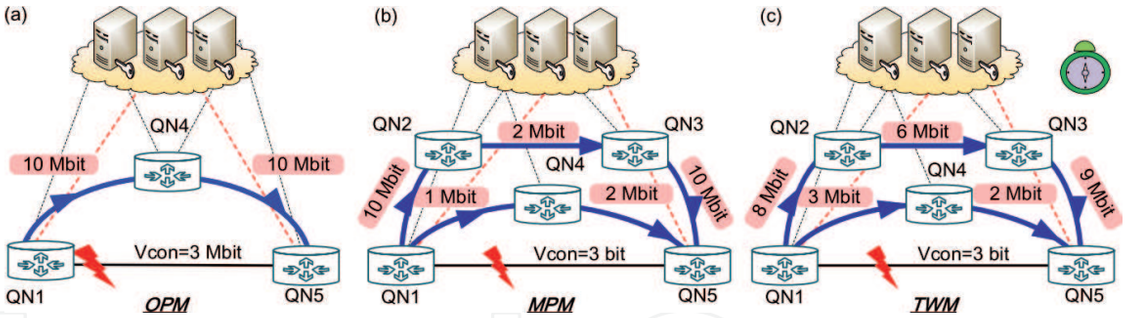

Figure 5.
Three methods. (a) OPM, (b) MPM, and (c) TWM [31].

Recovering and protecting failures for key provisioning services in QKDNs are an indispensable and vital problem to be solved.

In order to recover the key provisioning services affected by the failures in QKDNs, a Secret-Key Reallocation Strategy (SKRS) shown in **Figure 5(a)-(c)** is proposed including One-Path Method (OPM), Multi-Path Method (MPM) and Time-Window-based Method (TWM)) [31]. The strategy is to reallocate secret keys in QKPs and find available wavelengths, which are able to recover secret keys. By allocating the secret keys in QKPs over other paths, the security demand in failure-affected links will be satisfied. Multiple paths will try to provide keys simultaneously in case that the secret keys in one path are not enough. If multiple paths still fail to provide secret keys to meet the security demands, time division multiplexing technology can be considered. Simulation results verified that three proposed methods in the strategy can recover the failure-affected key provisioning services in different degree. Three methods of the strategy are as follows.

- **One-Path Method (OPM)**: The secret-key provisioning capability of a path P is denoted by secret-key volume (K_{low}) provided in P. The two failure-affected nodes are taken as the source and destination. Multiple paths are calculated as set P for the recovery. For each p in P, K_{low} is calculated, and whether path P can satisfy the security demands (K_d) is checked. Here, the unqualified paths will be removed from P, and the rest of the paths will be sorted in the decreasing order of K_{low}. Then, the strategy tries to find wavelength resources that are able to recover, and it stops once the enough required resources are found, when the link between QN1 and QN5 fails, path QN1- > QN4- > QN5 will be chosen to provide the secret-key and wavelength resources, which is shown in **Figure 5(a)**. If no path is found, go to MPM.

- **Multi-Path Method (MPM)**: MPM uses multiple paths as a group to recover the failed key distribution services. Different from OPM, MPM needs to check whether the sum of K_{low} in set P can meet the security demands K_d. If so, OPM takes the paths that satisfy the K_d as the candidate recovery paths; otherwise, go to TWM. In case that no single path has secret-key provisioning capability, two paths QN1- > QN4- > QN5 and QN1- > QN2- > QN3- > QN5 jointly provide secret keys, which is shown in **Figure 5(b)**.

- **Time-Window-based Method (TWM)**: TWH retries the steps in the OPM and MPM since the volume of existing secret keys changes over time. The OPM and MPM are executed during the time window until they are successful.

4.1 Machine learning application in QKDN

Machine learning (ML) is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. In recent years, a huge amount of attention on ML has been attracted from both the academia and the industry. There has been much development related to ML technologies in both hardware and software. More on-board acceleration chips for neural networks are implemented by new low-power devices.

Due to the advantages of ML, ML can help to solve several problems in QKDN. In terms of parameter optimization for QKD, ML can greatly improve the efficiency of parameter optimization and allow it to be performed in real time on low-power devices, making it a highly useful tool for both free-space QKD and QKD networks. In terms of key resource utilization, the effectiveness of using reinforcement learning to realize resource allocation in QKD networks is verified, which was published by Asia Communications and Photonics Conference (ACP) 2020 and honored as the best paper award in industry innovation [32]. As for the standardization activities, *P* recommendation ITU-T Y.QKDN-qos-ml-req "Requirements of machine learning based QoS assurance for quantum key distribution networks" specifies the functional mechanisms of machine-learning-based quality of service (QoS) assurance for QKDN; the supplement ITU-T Y.supp.QKDN-mla "ITU-T Y.3800-series - Quantum key distribution networks - Applications of machine learning" specifies different application scenarios of ML in QKDN. In detail, the applications of ML in QKDN include the applications in the quantum layer, key management layer, and QKDN control and management layers of QKDN.

- **The applications of ML in the quantum layer of QKDN** represent applying the ML to improve the performance of the quantum layer such as the quantum channel performance: (1) ML-based quantum channel performance prediction method will predict the quantum channel performance according to different channel environments. Through the predictions, the quantum channel will be in the optimal performance state in real time. Measures can be taken in advance to improve the channel environment to reduce unnecessary losses. (2) ML-based QKD system parameter optimization solution will optimize the QKD system quickly and accurately based on the real-time changing environment, maintaining the QKD system in the optimal performance state in real time. (3) ML-based RUL prediction of components in a QKD system solution will accurately estimate the RUL of components, which greatly improves the operability of the components and provides a guarantee for the normal QKD system operations.

- **The applications of ML in the key management layer of QKDN** represent applying the ML in the key management layer and improving the key management efficiency and stability: (1) ML-based key formatting solution will reduce the time cost and the risk of key synchronization failure during the key consumption by guiding the key formatting with the awareness of service characteristics before storing keys. (2) ML-based key storage management solution will evaluate and predict health state of key storage and help to realize the efficient utilization of key resources. (3) ML-based suspicious behavior detection in the key management layer will improve the efficiency of suspicious behavior detection and achieve great authentication accuracy.

- **The applications of ML in the control and management layers of QKDN** represent applying the ML in the control and management layers and improving the QKDN management and control efficiency: (1) The ML-based data collection and data preprocessing will collect and preprocess multi-source, heterogeneous QKDN data in an efficient way. The collected and preprocessed data will be transformed into understandable, unified, and easy-to-use structures and optimized in the form of balanced characteristics for subsequent procedures. (2) ML-based routing solution will improve the routing effectiveness and the key resources utilization. (3) The ML-based QKDN fault diagnosis solution will reduce the loss and avoid the risk of QKDN faults by realizing fault location and fault prediction.

5. Quantum teleportation network

Quantum teleportation (QT) is a quantum information transmission method that uses the uncertain properties of quantum entanglement to realize the remote transmission of quantum states. This part will introduce the existing research about QTNs briefly, including the point-to-point QT mechanism and multi-Hop QT networking mechanism.

5.1 Point-to-point QT mechanism

Point-to-Point QT mechanism [33] is based on quantum entanglement exchange [34]. The basic principle of quantum entanglement exchange is as follows: The purpose of quantum entanglement exchange is to generate quantum entanglement between quantum systems that have never directly interacted through certain physical processes. Entanglement swapping has great application prospects in quantum communication and quantum information networks, such as preparing entanglement and extending the distance of quantum communication [35]. As **Figure 6** shows, suppose particles A, B and particles C, D are two sets of EPR entangled pairs, respectively. Performing the Bell basis joint measurement of particles B and C, particles A and D is also in an entangled state and is in the same entangled state

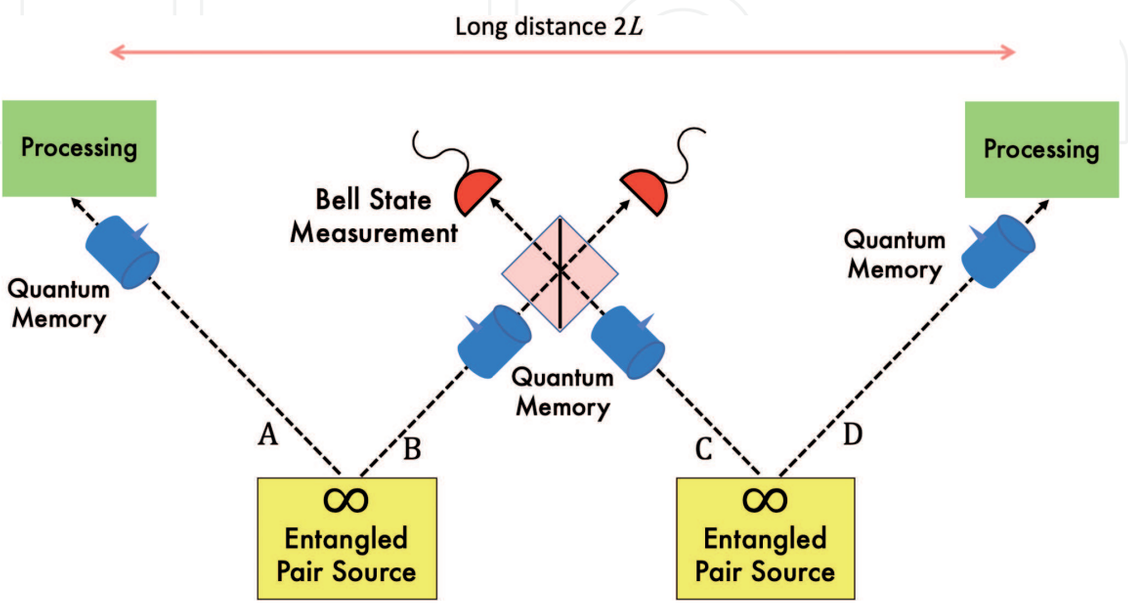

Figure 6.
Example of a one-hop, first-generation quantum repeater [36].

as particles 2 and 3, so that the entanglement exchange is successfully realized, and the point-to-point QT mechanism is completed.

5.2 Multi-hop QT networking mechanism

In a QTN based on teleportation, the necessary conditions for the transmission of information-carrying quantum states between two nodes are: a quantum channel composed of entangled particle pairs must exist between the source node and the destination node. However, it is impossible for any two nodes in the network to share entangled particle pairs, which means that the source node may not be able to directly transmit information to any other node in the network. In order to achieve communication between remote nodes, intermediate nodes are introduced to assist in the transmission of information [18]. Therefore, when the sender and the receiver directly share the entangled particle pair, the two nodes can directly transmit the quantum state; otherwise, there needs to be at least a quantum path established between the sender and the receiver—a quantum path established through an intermediate node. Entangled particle pairs are shared between neighboring nodes. The method of using teleportation technology to achieve quantum information transmission through intermediate nodes is called multi-hop QT [37].

In the traditional multi-hop QT system, the hop-by-hop QT scheme is often used. In the hop-by-hop QT transmission process, it is necessary to measure the entanglement of the nodes on the path one by one. According to the measurement result of the previous node, perform a unitary transformation on the particles held by the node to restore to the quantum state to be transmitted. The transmission of quantum information is from the source node to the destination node. An efficient multi-hop QT scheme is proposed [37]. The measurement results of the source node and the intermediate node are uniformly transmitted to the destination node, and only the unitary transformation is performed at the destination node.

6. Open issues in quantum communication networks

In recent years, the experimental research [15, 20, 38, 39] of quantum entanglement has mainly focused on how to expand the entanglement distribution distance, and the construction of quantum communication networks is mostly based on simple network topologies, mainly point-to-point network topologies, and a small number of star or bus network topology containing several nodes. There is little research on quantum communication networks under complex network structures, and research work should also be concentrated in the field of network security and quantum state transmission. Few works [40] have studied entanglement distribution from the level of quantum communication networks, so it is urgent and challenging to realize the connectivity of quantum communication network, repeating, switching, and routing quantum communication network and multi-layer quantum communication network.

- Connectivity of quantum communication network. How to deploy entangled particles and the location of distribution nodes play a vital role in the connectivity of the network. However, most of the current quantum communication network construction work is based on simple network topologies, mainly point-to-point network topologies, and a small number of star or bus network topologies that contain several nodes. There is little research on quantum communication networks under complex network structures, and research work is mainly focused on the field of network security and quantum state transmission, and the research on how to improve network connectivity is still insufficient.

- Repeating, switching, and routing quantum communication network. For the collaborative planning of the QT network, the main goal is to create relays, switches, and routes for quantum entanglement. The physical and software solutions in traditional networks are not suitable for quantum networks. The challenges they face include different forms of quantum entanglement generation and exchange, multi-user purification protocols, fusion and coordinated control, operation of traditional networks and quantum networks. To distribute entangled pairs between fixed target pairs, quantum repeaters need to be used to extend the distribution distance of entangled pairs. Unlike the operation of classical repeaters, quantum repeaters do not amplify photons in an entangled state during photon transmission. On the contrary, the quantum repeater can "jump" the entanglement property in the extra distance interval by consuming the resources of the second entangled pair. The innovation to achieve this is the quantum process of entanglement swapping.

- Multi-layer quantum communication network. The current quantum communication experiments rely on a set of devices with limited functionality and performance. However, to create wide-area and operational quantum networks, we need more capable devices with additional functionality. The devices are required to satisfy suitable requirements for reliability, scalability, and maintenance. Essential network devices to construct QTN include quantum memory, quantum switches, multiplexing technologies, transducers for quantum sources. Quantum memory should be improved with efficient optical interface and satellite-to-fiber connections; quantum switches should have high speed and low loss; transduction including microwaves is required, which is from optical and telecommunications regimes to quantum computer-relevant domain. Designing a quantum internet prototype capable of performing the aforementioned tasks will require developing a new quantum-updated version of the network stack.

7. Conclusions

In this chapter, the technologies to realize multipoint-interconnected quantum communication networks are summarized. Quantum communication enabling technologies including point-to-point QKD technologies and QT technologies are the basis to construct multipoint-interconnected quantum communication networks. As two typical quantum communication networks, quantum key distribution network (QKDN) and QT network are introduced respectively. In order to interconnect multiple points in QKDN, four sub-problems (i.e., architecture of QKDN, key supply in QKDN, resilience of QKDN, and machine learning in QKDN) are addressed. The architecture in QKDN consists of four planes: application (app) plane, control plane, QKD plane, and data plane, in top-down order. Key supply in QKDN needs a reasonable quantum key pooling mechanism and a balanced key resource scheduling strategy. Resilience of QKDN includes three methods to recover the failure-affected key provisioning services in different degrees. In order to interconnect multiple points in QT network, the existed research mainly pays attention on point-to-point QT mechanism and multi-hop QT networking mechanism, only few works have studied entanglement distribution from the multipoint interconnection of QT networks. Some open issues in quantum communication networks are also discussed, such as connectivity of quantum communication networks and how to plan quantum communication networks collaboratively.

Author details

Qingcheng Zhu, Yazi Wang, Lu Lu, Yongli Zhao*, Xiaosong Yu, Yuan Cao and Jie Zhang
State Key Laboratory of Information Photonics and Optical Communication, Beijing University of Posts and Telecommunications, Beijing, China

*Address all correspondence to: yonglizhao@bupt.edu.cn

IntechOpen

References

[1] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: IEEE International Conference on Computers, Systems and Signal Processing; 9-12 December 1984; Bangalore, India; Theoretical Computer Science. Vol. 560. 2014. pp. 175-179

[2] Yuan Z, Plews A, Takahashi R, Doi K, Tam W, Sharpe A, et al. 10-Mb/s quantum key distribution. Journal of Lightwave Technology. 2018;**36**(16): 3427-3433

[3] Tobias EA, Takuya H, Benjamin P, Georg R, Ruben L, Mikio F, et al. Wavelength division multiplexing of 194 continuous variable quantum key distribution channels. Journal of Lightwave Technology. 2020;**38**(8):2214-2218. DOI: 10.1109/JLT.2020.2970179

[4] Yin H, Chen T, Yu Z, Liu H, You L, Zhou Y, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Physical Review Letters. 2016;**117**(9):190501

[5] Chai G, Huang P, Cao Z, Zeng G. Suppressing excess noise for atmospheric continuous-variable quantum key distribution via adaptive optics approach. New Journal of Physics. 2020;**22**(10):103009

[6] Zhou X, Zhang C, Guo G, Wang Q. Improved decoy-state measurement-device-independent quantum key distribution with imperfect source encoding. IEEE Photonics Journal. 2019;**11**(3):7600207

[7] Peev M, Pacher C, Alléaume R, et al. The SECOQC quantum key distribution network in Vienna. New Journal of Physics. 2009;**11**:075001

[8] Aguado A, Lopez V, Lopez D, et al. The engineering of software-defined quantum key distribution networks. IEEE Communications Magazine. 2019;**57**(7):20-26

[9] Chen Y, Zhang Q, Chen T, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature. 2021;**589**(7841): 214-219

[10] Cao Y, Yongli Zhao YW, Xiaosong Y, Zhang J. Time-scheduled quantum key distribution (QKD) over WDM networks. IEEE/OSA Journal of Lightwave Technology. 2018;**36**(16):3382-3395

[11] Piparo LN, Razavi M. Long-distance trust-free quantum key distribution. IEEE Journal of Selected Topics in Quantum Electronics. 2014;**21**(3):123-130

[12] Guo Y et al. Quantum relay schemes for continuous-variable quantum key distribution. Physical Review A. 2017; **95**(4):042326

[13] de Riedmatten H, Marcikic I, Tittel W, Zbinden H, Collins D, Gisin N. Long distance quantum teleportation in a quantum Relay configuration. Physical Review Letters. 2004;**92**(4):1-4

[14] Guo D, Liu X, Ma Y, Xiao L, Long G. A theoretical scheme for multi-user quantum key distribution with N Einstein-Podolsky-Rosen pairs on a passive optical network. Chinese Physics Letters. 2002;**19**(7):893-896

[15] Yonezawa H, Aoki T, Furusawa A. Demonstration of a quantum teleportation network for continuous variables. Nature. 2004;**431**:430-433

[16] Bennett CH et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters. 1993;**70**(13):1895-1899

[17] Bouwmeester D et al. Experimental quantum teleportation. Nature. 1997;**390**:6660, 575-579

[18] Sun QC, Mao YL, Chen SJ, et al. Quantum teleportation with independent sources and prior entanglement distribution over a network. Nature Photonics. 2016;**10**(10):671-675

[19] Valivarthi R, Zhou Q, Aguilar GH, et al. Quantum teleportation across a metropolitan fibre network. Nature Photonics. 2016;**10**(10):676-680

[20] Pirandola S, Eisert J, Weedbrook C, et al. Advances in quantum teleportation. Nature Photon. 2015;**9**:641-652

[21] Kwiat PG et al. New high-intensity source of polarization-entangled photon pairs. Physical Review Letter*s*. 1995; **75**(24):4337

[22] Fejer MM et al. Quasi-phase-matched second harmonic generation: Tuning and tolerances. IEEE Journal of Quantum Electronics. 1992;**28**(11): 2631-2654

[23] Fulconis J et al. Nonclassical interference and entanglement generation using a photonic crystal fiber pair photon source. Physical Review Letters. 2007;**99**(12):120501

[24] Zhao Y, Cao Y, Wang W, Wang H, Yu X, Zhang J, et al. Resource allocation in optical networks secured by quantum key distribution. IEEE Communications Magazine. 2018;**56**(8):130-137

[25] Lo H-K et al. Secure quantum key distribution. Nature Photonics. 2014;**8**:595-604

[26] Peev M et al. The SECOQC quantum key distribution network in Vienna. New Journal of Physics. 2009;**11**(7): 075001.1-075001.07500137

[27] Quantum Safe Cryptography and Security. ETSI White Paper No. 8, June 2015 [Online]. Available from: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[28] Cao Y, Zhao Y, Wang J, Yu X, Ma Z, Zhang J. Cost-efficient quantum key distribution (QKD) over WDM networks. IEEE/OSA Journal of Optical Communications and Networking. 2019;**11**(6):285-298

[29] Cao Y, Zhao Y, Wang J, Yu X, Ma Z, Zhang J. KaaS: Key as a service over quantum key distribution integrated optical networks. IEEE Communications Magazine. 2019;**57**(5):152-159

[30] Cao Y, Zhao Y, Colman-Meixner C, Yu X, Zhang J. Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). Optics Express. 2017;**25**(22): 26453-26467

[31] Wang H, Zhao Y, Yu X, Chen B, Zhang J. Resilient Fiber-based Quantum Key Distribution (QKD) Networks with Secret-key Re-allocation Strategy. San Diego, CA, USA: OFC2019; 2019

[32] Zuo Y, Zhao Y, Yu X, Nag A, Zhang J. Reinforcement Learning-based Resource Allocation in Quantum Key Distribution Networks. Beijing, China: ACP/IPOC2020; 2020

[33] Huo M et al. Deterministic quantum teleportation through fiber channels. Science Advances. 2018;**4**(10):eaas9401

[34] Pirandola S. End-to-end capacities of a quantum communication network. Communications Physics. 2019;**2**(51)

[35] Jun Y. The Research on Quantum Teleportation of Quantum Communication. Huazhong University of Science and Technology; 2007

[36] Kleese van Dam K. From Long-distance Entanglement to Building a Nationwide Quantum Internet: Report

of the DOE Quantum Internet Blueprint Workshop. No. BNL-216179-2020-FORE. Upton, NY (United States): Brookhaven National Lab. (BNL); 2020

[37] Zhenzhen Z. Research on Multi-Hop Transmission and Networking for Quantum Communication Network. Southeast University; 2018

[38] Valivarthi R, Puigibert M, Zhou Q, et al. Quantum teleportation across a metropolitan fibre network. Nature Photon. 2016;**10**:676-680

[39] van Loock P, Braunstein SL. Multipartite entanglement for continuous variables: A quantum teleportation network. Physical Review Letters. 2000;**84**:3482

[40] Joshi SK et al. A trusted node–free eight-user metropolitan quantum communication network. Science Advances. 2020;**6**(36):eaba0959