Hybrid Trusted/Untrusted Relay Based Quantum Key Distribution over Optical Backbone Networks

Yuan Cao, Yongli Zhao, *Senior Member, IEEE,* Jun Li, Rui Lin, Jie Zhang, and Jiajia Chen, *Senior Member, IEEE*

***Abstract*—Quantum key distribution (QKD) has demonstrated a great potential to provide future-proofed security, especially for 5G and beyond communications. As the critical infrastructure for 5G and beyond communications, optical networks can offer a cost-effective solution to QKD deployment utilizing the existing fiber resources. In particular, measurement-device-independent QKD shows its ability to extend the secure distance with the aid of an untrusted relay. Compared to the trusted relay, the untrusted relay has obviously better security, since it does not rely on any assumption on measurement and even allows to be accessed by an eavesdropper. However, it cannot extend QKD to an arbitrary distance like the trusted relay, such that it is expected to be combined with the trusted relay for large-scale QKD deployment. In this work, we study the hybrid trusted/untrusted relay based QKD deployment over optical backbone networks and focus on cost optimization during the deployment phase. A new network architecture of hybrid trusted/untrusted relay based QKD over optical backbone networks is described, where the node structures of the trusted relay and untrusted relay are elaborated. The corresponding network, cost, and security models are formulated. To optimize the deployment cost, an integer linear programming model and a heuristic algorithm are designed. Numerical simulations verify that the cost-optimized design can significantly outperform the benchmark algorithm in terms of deployment cost and security level. Up to 25% cost saving can be achieved by deploying QKD with the hybrid trusted/untrusted relay scheme while keeping much higher security level relative to the conventional point-to-point QKD protocols that are only with the trusted relays.**

***Index Terms*—Measurement-device-independent quantum key distribution, optical networks, security, cost optimization.**

I. Introduction

In the next generation networks, an enormous amount of confidential data and sensitive information will be transferred to support 5G and beyond applications. However, significant technical breakthroughs have been achieved in developing quantum computers [1], [2], threatening the standard cryptographic methods that are widely employed in today's communication networks. In this regard, providing security and privacy becomes a rigorous challenge [3], [4]. An effective method to overcome this challenge is quantum key distribution (QKD) [5]–[7], since it promises key exchange with information-theoretic security by utilizing the quantum nature of information. Accordingly, QKD holds the potential of providing long-term protection and future-proofed security for 5G and beyond communications.

QKD enables two remote parties to share secret keys in a point-to-point fashion. It is important to note that amplifying quantum signals is impossible since the quantum no-cloning theorem [8] proves that an unknown quantum state cannot be cloned. Thus, the distance of QKD is limited due to the unavoidable photon loss during quantum-signal propagation. Recently, significant technical advances have been made in the theory and experiment of point-to-point QKD over the optical fiber [9] and free space [10]. Commercially, fiber-based QKD systems are available on the market today, which are developed based on conventional point-to-point QKD protocols, such as Bennett-Brassard-1984 (BB84) [11], coherent-one-way (COW) [12], and Grosshans-Grangier-2002 (GG02) [13].

Many fiber-based QKD networks [7], [14]–[16] have been deployed in the field. A QKD network consists of two or more QKD nodes interconnected by fiber links. Previously, the dark fiber was utilized for quantum-signal transmission in order to protect the fragile quantum signals from the negative impact of intense classical signals. However, dark fibers are expensive and scarce resources, making the practical deployment of QKD networks difficult and costly. Meanwhile, deploying new fiber infrastructures for QKD networking is time consuming and costly. Thanks to the advances in quantum-classical coexistence schemes based on wavelength-division multiplexing (WDM), the recent in-field demonstrations in Cambridge [17] and Madrid [18] have implemented the coexistence of quantum and classical signals in the same fiber, allowing QKD over the existing optical networks. Hence, optical networks can offer a cost-effective solution to QKD deployment utilizing the legacy fiber infrastructure, while QKD can fulfil the high security demands of numerous services for 5G and beyond.

Generally, QKD networks can be realized based on three techniques, i.e., optical switching, trusted relay, and quantum repeater. Today, the practical QKD networks deployed in the field are based on the former two techniques. Despite technical advances made in quantum repeaters [19]–[22], the practical deployment in the field has not yet been realized. Optical switching technique exploits the classical optical functions to enable the switching of quantum channels, but it is only suitable for small-scale networks such as access [23] and relatively

Manuscript received July 15, 2020; revised November 24, 2020. This work was supported in part by National Key Research and Development Program of China (2020YFE0200600), National Natural Science Foundation of China (62021005, 61822105), Fundamental Research Funds for the Central Universities (2019XD-A05), Swedish Research Council, Swedish Foundation for Strategic Research, Swedish Foundation for International Collaboration in Research and Higher Education, and GENIE Project funded by the Chalmers University of Technology Foundation. *(Corresponding author: Yongli Zhao.)*

Yuan Cao, Yongli Zhao, and Jie Zhang are with the State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: yuancao@bupt.edu.cn; yonglizhao@bupt.edu.cn; lgr24@bupt.edu.cn).

Jun Li, Rui Lin, and Jiajia Chen are with the Department of Electrical Engineering, Chalmers University of Technology, 412 96 Gothenburg, Sweden (e-mail: ljun@chalmers.se; ruilin@chalmers.se; jiajiac@chalmers.se).

small metropolitan networks [24] due to the limited achievable distance. In practice, long-distance QKD can be implemented based on the trusted relay technique [7], [25], where the local secret keys are stored in the trusted relays and forwarded in a hop-by-hop fashion to establish the global secret keys between source and destination nodes. It is important to note that all nodes are assumed trustable in a trusted relay based QKD network. Hence, the trusted relays constitute weak points of security in practice.

In recent years, measurement-device-independent QKD (MDI-QKD) has attracted much attention, which is able to extend the secure distance to some extent and close all detection loopholes (i.e., avoid any attacks against imperfect detectors in practical QKD systems) with the aid of an untrusted relay [26]. The untrusted relay has better security than the trusted relay, since the untrusted relay does not rely on any assumption on measurement and even allows to be accessed by an eavesdropper without affecting the security [27]. Recently, a field trial of MDI-QKD metropolitan network [27] and the coexistence of MDI-QKD with classical communications [28] have been implemented. Accordingly, the deployment of MDI-QKD over optical networks has become a feasible solution. MDI-QKD has the power to double the secure distance that can be achieved by conventional point-to-point QKD protocols [26]. However, the achievable distance by using the untrusted relay alone is still limited to $\sim$500 km [29], [30] with the state-of-the-art phase-encoding MDI-QKD protocols. As directly connecting two untrusted relays is not allowed, trusted relays need to be introduced which can extend QKD distance without constraints. Hence, the untrusted relay is expected to be used in synergy with the trusted relay for the deployment of a large-scale QKD network. Such a network has a great potential to possess a higher level of security in practice owing to the reduced number of trusted relays compared to the QKD networks based on purely trusted relays [7], [25].

Nevertheless, how to achieve the optimal deployment of hybrid trusted/untrusted relay based QKD over existing optical backbone networks needs to be explored. In this work, we address this research problem and concentrate on cost optimization during the deployment phase. Our main contributions are summarized as follows:

- We introduce a new network architecture of hybrid trusted/untrusted relay based QKD over optical backbone networks to support high security required by emerging 5G and beyond applications, in which the node structures of the trusted relay and untrusted relay are elaborated.
- We formulate a new cost model for deploying QKD with hybrid trusted/untrusted relays over an existing optical backbone network, where the deployment costs of various network components are considered.
- We devise an integer linear programming (ILP) model and a heuristic algorithm to optimize the deployment cost.
- We evaluate the performance through numerical simulations, and perform a comparative analysis of the hybrid trusted/untrusted relay and purely trusted relay schemes in terms of deployment cost, network component usage, and security level.
- We discuss some open issues on hybrid trusted/untrusted relay based QKD over optical backbone networks for future research.

The rest of this paper is organized as follows. Section II reviews the related work for QKD over optical networks that are able to greatly support high security for 5G and beyond applications. Section III describes the network architecture and node structures. The corresponding network, cost, and security models are formulated in Section IV. The ILP model and heuristic algorithm are presented in Sections V and VI, respectively. Section VII carries out the performance evaluation and analysis through extensive simulations. Some open issues in future research are discussed in Section VIII. Finally, Section IX gives the conclusion.

II. Related Work

This section reviews related work on the network aspects of QKD over optical networks. Integrating QKD with optical networks is able to offer high security to 5G and beyond applications. The physical layer aspects are not elaborated here since the focus of this paper is on the network aspects.

With respect to the resource allocation for different channels (e.g., quantum and classical channels) in a QKD-integrated optical network, machine learning methods have been adopted for optimal channel allocation through real-time prediction [31], [32], thereby the sufficient secret-key rate is guaranteed in real time. In [33]–[35], time-division multiplexing technique was brought in a QKD-over-WDM network to improve the resource utilization for both quantum and classical channels. The offline resource allocation problem has been addressed with the ILP model and heuristics [33], [34], while the online version has been solved using heuristics [35]. In [36], several near-optimal wavelength allocation schemes were designed to improve the achievable secret-key rates, where different physical-layer impairments were considered. In particular, software defined networking (SDN) techniques can be utilized to enhance the flexibility of channel allocation and configuration in a QKD-integrated optical network, which has been demonstrated through experiments [37] and field trials [18], [31], [38].

From the perspective of QKD network applications, several potential service provisioning ways such as key on demand [39], multi-tenancy [40]–[42], QKD as a service [43], and quality-of-service provisioning [44] have been presented to offer high security. A variety of use cases have demonstrated the application of QKD networks in the security domain, such as the security enhancement of the 5G service orchestration [45], the virtual optical network [46], and the multicast services [47]. Massive confidential data and sensitive information from 5G and beyond applications are transported through optical networks, whose ultimate security and privacy are promising to be enhanced by QKD [4]. In addition, the control plane in SDN and network function virtualization environments can be secured by QKD networks [39], [48].

In particular for the optimal deployment of QKD networks, Alléaume *et al.* [49] investigated the QKD network deployment from a topology perspective, where some analytical models were presented to optimize the spatial distribution of

QKD nodes. However, dedicated dark fibers were considered for QKD deployment instead of relying on existing optical networks. In [50], a cost-efficient design was performed for deploying QKD over WDM networks, in which an ILP model and a heuristic algorithm were developed to achieve cost-efficient QKD backbone network deployment. In [51], the optimal design of deploying QKD for securing optical transport networks was studied, where two mixed ILP models were formulated and evaluated through simulations. Nevertheless, the existing work [49]–[51] only focused on the optimal deployment of QKD with purely trusted relays.

In fact, inspired by the technical advances in MDI-QKD [27]–[30] that allows the use of the untrusted relay, the optimal deployment of QKD with hybrid trusted/untrusted relays needs to be investigated. Recently, the routing problem in a hybrid trusted/untrusted relay based QKD network has been studied [52]. To the best of our knowledge, the cost optimization for the deployment of such a new QKD network paradigm has yet to be addressed.

III. Network Architecture and Node Structure

In this section, we describe a network architecture of hybrid trusted/untrusted relay based QKD over optical backbone networks, as illustrated in Fig. 1. This architecture comprises two layers, i.e., QKD layer and optical layer. In practice, control and application layers can be added on top as the upper layers to implement the control, management, and orchestration of QKD and optical networks, as well as to realize the secure service provisioning. Such a multi-layer architecture can refer to [35], [45], [46], and this work focuses on QKD and optical layers that are elaborated in the following paragraphs. Table I lists the abbreviations and their definitions used in this paper.

In the QKD layer, as MDI-QKD is considered, a hybrid trusted/untrusted relay based QKD backbone network is deployed. Three types of QKD nodes (i.e., QKD backbone node, trusted relay, and untrusted relay) are needed. A QKD backbone node acts as the end node to supply secret keys to its co-located optical backbone node. The untrusted relay and trusted relay act as the intermediate nodes between a pair of QKD backbone nodes. The specific node structures of the trusted relay and untrusted relay are depicted in Fig. 2. An untrusted relay comprises one or more MDI-QKD receivers (MDI-QRxs). A trusted relay contains two or more MDI-QKD transmitters (MDI-QTxs), a local key manager (LKM) [53], and the security infrastructure (SI) [49]. A pair of connected MDI-QTxs can only generate the local secret keys if there is an MDI-QRx between them. The MDI-QKD protocol needs to be realized with two MDI-QTxs and one MDI-QRx, and the MDI-QRx should be placed between the two MDI-QTxs [26]. The secret keys cannot be generated without the MDI-QRx. Therefore, between a pair of connected MDI-QTxs, one untrusted relay must be deployed, while more than one untrusted relay is not allowed. The LKM receives and stores the local secret keys from its connected MDI-QTxs, and performs secret-key relay with the one-time pad method [54] to produce global secret keys between a pair of QKD backbone nodes. The SI is used to ensure that the trusted relay

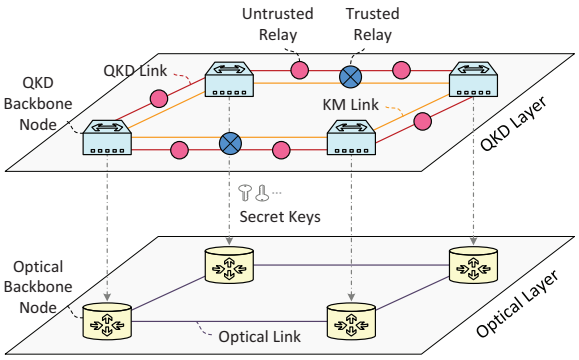


Fig. 1. Network architecture: hybrid trusted/untrusted relay based QKD over optical backbone networks.

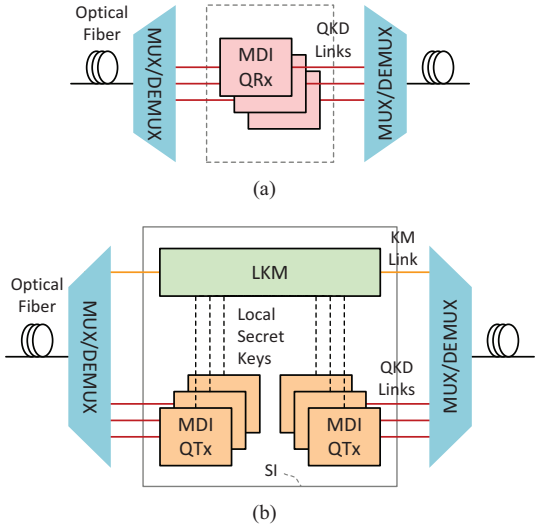


Fig. 2. Node structures: (a) untrusted relay; (b) trusted relay.

is physically installed and isolated in a secure environment. The LKM and its connected MDI-QTxs should be put in the SI.

The protocol that supports untrusted relay is the MDI-QKD protocol (for secret-key generation) realized by the MDI-QRx, while the protocols for the trusted relay are the MDI-QKD protocol (for secret-key generation) realized by the MDI-QTx and the one-time pad protocol (for secret-key relay) implemented at the LKM, respectively. The local secret keys are generated between a pair of connected MDI-QTxs, thus the trusted relays containing MDI-QTxs are weak security points in the QKD backbone network. Specifically, the secret keys might be eavesdropped at the trusted relays. According to the node structure of the untrusted relay shown in Fig. 2(a), an untrusted relay contains only the MDI-QRx and cannot access the secret keys. Therefore, the QKD backbone network is secure even if the untrusted relays are controlled by the eavesdropper.

With respect to different links in the QKD layer, MDI-QTxs and MDI-QRxs are interconnected by QKD links, while LKMs are interconnected by key management (KM) links. In general, a QKD link has both quantum and classical channels. The quantum channel is a physical link that can be carried out by

TABLE I
ABBREVIATIONS AND DEFINITIONS

Abbreviations	Definitions
QKD	Quantum Key Distribution
BB84	Bennett-Brassard-1984
COW	Coherent-One-Way
GG02	Grosshans-Grangier-2002
WDM	Wavelength-Division Multiplexing
MDI	Measurement-Device-Independent
ILP	Integer Linear Programming
SDN	Software Defined Networking
QTx	QKD Transmitter
QRx	QKD Receiver
LKM	Local Key Manager
SI	Security Infrastructure
KM	Key Management
MUX	Multiplexer
DEMUX	Demultiplexer
GKS	Global Key Server
EDFA	Erbium Doped Fiber Amplifier
CO-QBN	Cost-Optimized QKD Backbone Networking
SC/UC/DC	Static/Uniform/Dynamic Case
PTR	Purely Trusted Relay

a wavelength channel for quantum-signal transmission, and the classical channel is a logical link that can be realized by two or more wavelength channels for synchronization (unidirectional classical communication), distillation (bidirectional classical communication), and so on [53]. The other multiplexing techniques (e.g., time-division multiplexing) may be exploited to reduce the number of wavelength channels required for a QKD link, which are not considered in this work. A KM link is a logical link and only has the classical channel, which can also be implemented by a wavelength channel [25]. Specifically, the multiplexer/demultiplexer (MUX/DEMUX) components connected to trusted/untrusted relays can be utilized to multiplex/demultiplex different wavelength channels of QKD and KM links in the same fiber.

A QKD backbone node contains a global key server (GKS) and various devices of trusted/untrusted relays, which can also realize the functions of trusted/untrusted relays. The SI is also required to protect a QKD backbone node within the security perimeter. A GKS stores the produced global secret keys and manages their overall lifetime from production by LKMs to consumption by high-security-demand services. Moreover, the GKS can prestore a portion of global secret keys dedicated for resilience guarantee. Even if a network failure occurs, there are still available secret keys for protection purposes, enabling the QKD backbone network to be robust against various failures without adding additional devices/links.

Between any pair of QKD backbone nodes, a hybrid trusted/untrusted relay based QKD chain can be established to generate the global secret keys. As shown in Fig. 3(a), we use an example of such a QKD chain to further describe the functions of various devices and links in the QKD layer. A pair of connected MDI-QTxs in symmetric positions both send out encoded quantum signals to their connected MDI-QRx (in the untrusted relay) via a QKD link. Then, the MDI-QRx performs a Bell state measurement that projects the incoming quantum signals into a Bell state [26], and publicly announces the measurement results to correlate the key information of two MDI-QTxs. More details about the MDI-QKD protocol can refer to [26]. Finally, the local secret keys can be generated between such a pair of MDI-QTxs and stored in their connected LKMs. The symmetric position means that the two channels (e.g., Ch-a and Ch-b in Fig. 3) are symmetric with similar losses, that is, the two connected MDI-QTxs have symmetric distances to the untrusted relay. This symmetry was necessary in previous implementations of MDI-QKD [26], [27], since the secret-key rate is severely limited in the case where different channels have different losses. The requirement for symmetric channels can be fulfilled by deliberately adding a custom length of fiber to the shorter channel. On the other hand, the recent invention and demonstration of asymmetric protocols for MDI-QKD [55], [56] have offered a new way to compensate channel asymmetry. Therefore, MDI-QKD over both symmetric and asymmetric channels is feasible in practice.

As illustrated in Fig. 3(a), a string of secret keys K_{A} is shared between QKD Backbone Node 1 and Trusted Relay 1, while another string of secret keys K_{B} is shared between Trusted Relay 1 and QKD Backbone Node 2. In order to further extend the reach of QKD, additional interleaved trusted/untrusted relays can be added, and the LKM in each trusted relay can forward the secret keys in a hop-by-hop fashion along the QKD chain via a KM link. In an LKM, the one-time pad method is used for encryption to guarantee the information-theoretic security of secret keys. As an example, the LKM in Trusted Relay 1 combines K_{A} and K_{B} of the same string length with one-time pad method, namely, conducts a bitwise exclusive OR operation between K_{A} and K_{B}, and then sends $K_{\mathrm{A}} \oplus K_{\mathrm{B}}$ to the LKM in QKD Backbone Node 2 through a KM link. Based on $K_{\mathrm{B}} \oplus (K_{\mathrm{A}} \oplus K_{\mathrm{B}}) = K_{\mathrm{A}}$, the LKM in QKD Backbone Node 2 can retrieve K_{A}. Both the LKMs in QKD Backbone Nodes 1 and 2 will deliver K_{A} to their connected GKSs. Hence, K_{A} is shared between QKD Backbone Nodes 1 and 2, which is referred as the global secret key. In addition, it is possible that there is no trusted relay between some pairs of QKD backbone nodes. Such a case is illustrated in Fig. 3(b), where a string of secret keys K_{C} is shared directly between QKD Backbone Nodes A and B. The limitations of this case, however, are that the distance between a pair of QKD backbone nodes must be within the achievable distance between a pair of connected MDI-QTxs, and that only one untrusted relay is allowed between such a pair of QKD backbone nodes.

In Fig. 1, the optical layer consists of an optical backbone network. Such a network comprises a set of optical backbone nodes interconnected by optical links. In the optical backbone network, optical signals are amplified using the erbium doped fiber amplifiers (EDFAs) on the optical links in order to propagate a long distance. It is important to note that a QKD backbone node needs to be placed in the same physical location as an optical backbone node, such that the secret keys in QKD backbone nodes can be delivered to optical backbone

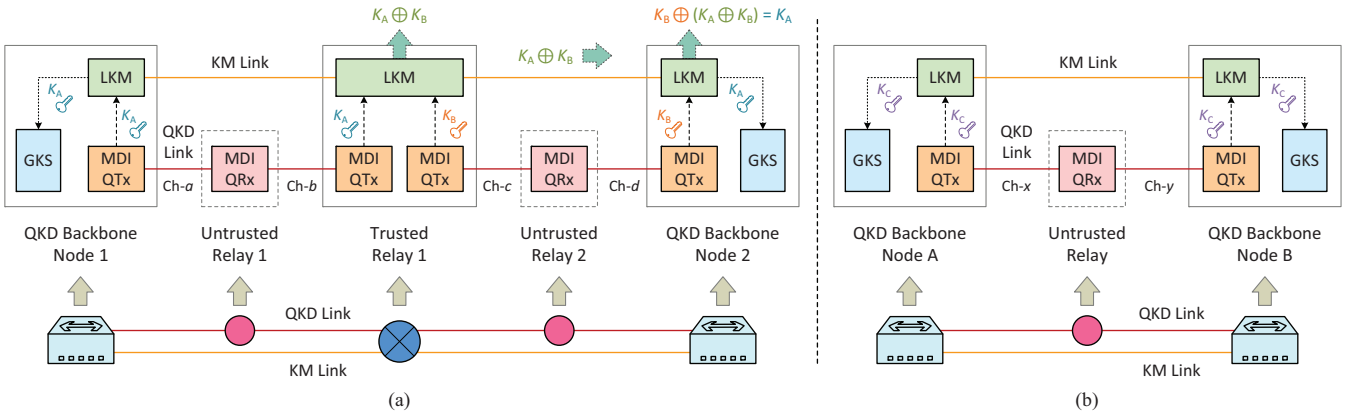


Fig. 3. Illustration of (a) a hybrid trusted/untrusted relay based QKD chain and (b) a special case of the QKD chain without using the trusted relay. (For simplicity, the logical connections are indicated and MUX/DEMUX components are not included)

nodes for fulfilling the high security demands of services.

Based on the WDM technique, the QKD, KM, and optical links can be multiplexed in the same fiber with MUX/DEMUX components. Meanwhile, the wavelength continuity needs to be considered for the QKD/KM links, since the same wavelength channel is required on the fiber links along the path of a QKD chain. In general, EDFAs are deployed on optical links approximately every 80 km. An EDFA bypass scheme [50], [57] can reduce the negative impact of the amplified spontaneous emission noise caused by EDFA on quantum signals, where additional MUX/DEMUX components are required to enable the quantum signals to bypass EDFA. If the trusted/untrusted relay is not deployed in the same physical location as the EDFA, the MUX/DEMUX components need to be added at both locations, namely the trusted/untrusted relay location (for multiplexing/demultiplexing QKD, KM, and optical links) and the EDFA location (for EDFA bypass). It means two MUX/DEMUX components are needed. When the untrusted relay or the trusted relay is deployed at the same physical location as the EDFA, one MUX/DEMUX component can be used for both EDFA bypass and multiplexing/demultiplexing QKD, KM and optical links, thereby saving one MUX/DEMUX component. To take such an advantage, in this work the trusted/untrusted relay is assumed to be co-located with the EDFA. This is also a preferable option for the hybrid trusted/untrusted relay based QKD deployment over optical backbone networks. Note that the MUX/DEMUX components are always required to multiplex/demultiplex QKD, KM, and optical links at the trusted/untrusted relay locations, as shown in Fig. 2.

To achieve secret-key relay, each chain segment links the adjacent two trusted relays or a QKD backbone node and a trusted relay under the MDI-QKD distance limitation (∼160 km considered in this paper, i.e., the trusted/untrusted relays are co-located with EDFAs). In practice, when the distance of the last chain segment is less than 80 km, an untrusted relay is still required to implement MDI-QKD. One option is to place this untrusted relay at the same physical location as the QKD backbone node, and connect it to the MDI-QTx via additional fibers if needed.

IV. Problem Formulation

In this section, we formulate the network, cost, and security models for deploying QKD with hybrid trusted/untrusted relays over an existing optical backbone network. The notations used in this paper are listed and defined in Table II.

A. Network Model

We assume that a QKD backbone node is co-located with an optical backbone node and different links are multiplexed in the same fiber. Accordingly, the topology for the QKD layer is the same as the topology for the optical layer. We model a backbone network topology as $G(N, L)$, where N and L represent the sets of optical/QKD backbone nodes and fiber links, respectively. The sets of wavelength channels available on each physical link for QKD links and KM links are denoted by W_{Q} and W_{M}, respectively. The QKD links contain both quantum and classical channels, while the KM links comprise only classical channels. Therefore, different wavelength sets need to be predetermined for QKD links and KM links, which is beneficial to avoid the mixed use of wavelengths for different types of channels. The detailed channel allocation scheme will be discussed in the next subsection. Let τ represent the distance between an MDI-QTx and its connected MDI-QRx. Hence, the distance between a pair of connected MDI-QTxs is defined as

$$D \approx 2 \cdot \tau \tag{1}$$

due to the fact that in general the positions of two connected MDI-QTxs are preferably symmetrical. Let K_D represent the maximum achievable secret-key rate at distance D between two connected MDI-QTxs. The value of K_D is inversely proportional to the distance D, that is, an increase in D will lead to a decrease in K_D [29], [30]. For a more general consideration, the specific value of K_D in terms of the bit rate is not considered in this work. This is because the achievable secret-key rate is affected not only by the distance (i.e., fiber length), but also by the fiber link performance (e.g., loss and noise). Especially when MDI-QKD is coexisting with classical optical communications, it is not universal to consider the specific variation of the achievable bit rate with distance for

TABLE II
NOTATIONS AND DEFINITIONS

Notations	Definitions
$G(N, L)$	Optical/QKD backbone network topology
N	Set of optical/QKD backbone nodes
L	Set of fiber links
i, j	Index of the adjacent optical/QKD backbone nodes in N
$l_{(i,j)}$	Physical length of a fiber link between i and j
W_{Q}	Set of available wavelength channels for QKD links
W_{M}	Set of available wavelength channels for KM links
τ	Distance between an MDI-QTx and its connected QRx
D	Distance between a pair of connected MDI-QTxs
K_D	Maximum achievable secret-key rate at distance D
$r(s_r, d_r, \eta_r)$	QKD chain request
s_r	Source QKD backbone node of r
d_r	Destination QKD backbone node of r
η_r	Number of parallel QKD links for fulfilling k_r
k_r	Secret-key rate requirement between s_r and d_r
p_r	Alternative path between s_r and d_r for r
L_r	Set of fiber links on the path of r
R	Set of QKD chain requests
ρ	A given parameter
α^r_{Tx}	Required number of MDI-QTxs for r
α^r_{Rx}	Required number of MDI-QRxs for r
α^r_{KM}	Required number of LKMs for r
α^r_{TR}	Required number of trusted relays for r
α^r_{MD}	Required number of MUX/DEMUX pairs for r
α^R_{TR}	Total number of trusted relays for all QKD chain requests
l^r_{Ch}	Physical length of QKD and KM links for r
γ^r_{Tx}	Cost of an MDI-QTx for r
γ^r_{Rx}	Cost of an MDI-QRx for r
γ^r_{KM}	Cost of an LKM for r
γ^r_{SI}	Cost of the SI for a trusted relay of r
γ^r_{MD}	Cost of a pair of MUX/DEMUX components for r
γ^r_{Ch}	Cost per kilometer of a wavelength channel for r
C^R_{Tx}	Cost of MDI-QTxs for all QKD chain requests
C^R_{Rx}	Cost of MDI-QRxs for all QKD chain requests
C^R_{KM}	Cost of LKMs for all QKD chain requests
C^R_{SI}	Cost of SIs for all QKD chain requests
C^R_{MD}	Cost of MUX/DEMUX for all QKD chain requests
C^R_{Ch}	Cost of links for all QKD chain requests
C^R_{Total}	Total deployment cost
SL_R	Security level of the QKD backbone network
$f^r_{(i,j),\lambda}$	Boolean variable that equals 1 if wavelength λ on link (i, j) is assigned to the QKD link of r, and 0 otherwise
$x^r_{(i,j),w}$	Boolean variable that equals 1 if wavelength w on link (i, j) is assigned to the KM link of r, and 0 otherwise
K	Number of alternative paths in K-*shortest-path* algorithm

MDI-QKD. In order to achieve a secret-key rate at the level of kbps and facilitate EDFA bypass, the value of D considered in this paper is ∼160 km (i.e., the trusted/untrusted relays are co-located with EDFAs). As described in Section III, some special circumstances, e.g., MDI-QKD over asymmetric channels and a fiber length of less than 80 km for the last chain segment, are also incorporated in the network model.

A QKD chain based on the hybrid trusted/untrusted relays is established between a pair of QKD backbone nodes to fulfil the high security demands of services between the corresponding two optical backbone nodes. We model a QKD chain request as $r(s_r, d_r, \eta_r)$, where s_r and d_r denote the source and destination QKD backbone nodes of r, and η_r is the number of parallel QKD links for fulfilling the secret-key rate requirement between s_r and d_r. This is because multiple parallel QKD links can be multiplexed in the same fiber to reach a higher secret-key rate than the maximum achievable secret-key rate on a single QKD link [58]. The parameter η_r can be defined as

$$\eta_r = \left\lceil \frac{k_r}{K_D} \right\rceil \tag{2}$$

where k_r represents the secret-key rate requirement between s_r and d_r. The specific secret-key rate requirement of each QKD chain is not considered in this work. Even though the distance (i.e., fiber length) between each pair of connected MDI-QTxs is the same (e.g., ∼160 km), the achievable secret-key rate can still be different due to different losses and noises. Instead, the required number of parallel QKD links is considered as an input that reflects the secret-key rate requirement of each QKD chain. For example, $\eta_r = 1$ represents that one MDI-QRx and two MDI-QTxs are required in an untrusted relay and a trusted relay for r, respectively; while $\eta_r = 2$ represents that two MDI-QRxs and four MDI-QTxs are required in an untrusted relay and a trusted relay for r, respectively. The added two MDI-QTxs and one MDI-QRx are utilized to fulfil the higher secret-key rate requirement. Hence, η_r is a positive integer, which may be different for various QKD chain requests. In practice, $\eta_r = 1$ has been considered in many QKD networks with purely trusted relays (e.g., Beijing-Shanghai QKD backbone network [7]).

The set of QKD chain requests during the deployment phase is denoted by R. Based on the network topology, a given parameter ρ is denoted as

$$\rho = \frac{|N| \cdot (|N| - 1)}{2} \tag{3}$$

which can represent the total number of QKD chain requests when any QKD backbone node pair hosts one request.

B. Cost Model

The cost comes from various network components (e.g., devices and links) that need to be deployed to support QKD with hybrid trusted/untrusted relays over an existing optical backbone network, which will be detailed as follows.

1) Cost of MDI-QTxs and MDI-QRxs: In this study, we adopt only one type of QKD transceiver (i.e., MDI-QTx and MDI-QRx) to implement QKD throughout the network, while other QKD transceivers based on conventional point-to-point QKD protocols (e.g., BB84, COW, and GG02) are not considered. Due to the fact that an MDI-QKD process requires two MDI-QTxs and one MDI-QRx, the required numbers of MDI-QTxs and MDI-QRxs for a QKD chain request r can be formulated as

$$\alpha^r_{\mathrm{Tx}} = \sum_{(i,j)\in L_r} 2 \cdot \eta_r \cdot \left\lceil \frac{l_{(i,j)}}{D} \right\rceil \tag{4}$$

$$\alpha_{\mathrm{Rx}}^{r} = \sum_{(i,j)\in L_r} \eta_r \cdot \left\lceil \frac{l_{(i,j)}}{D} \right\rceil \tag{5}$$

where $l_{(i,j)}$ is the physical length of a fiber link between the adjacent QKD backbone nodes i and j, as well as L_r is the set of fiber links on the path of r. Based on (4) and (5), the costs of MDI-QTxs and MDI-QRxs for all QKD chain requests can be formulated as

$$C_{\mathrm{Tx}}^{R} = \sum_{r\in R} \gamma_{\mathrm{Tx}}^{r} \cdot \alpha_{\mathrm{Tx}}^{r} \tag{6}$$

$$C_{\mathrm{Rx}}^{R} = \sum_{r\in R} \gamma_{\mathrm{Rx}}^{r} \cdot \alpha_{\mathrm{Rx}}^{r} \tag{7}$$

where γ_{Tx}^{r} and γ_{Rx}^{r} represent the costs of an MDI-QTx and an MDI-QRx for the QKD chain request r, respectively.

2) Cost of LKMs: For each QKD chain, an LKM is required in both the trusted relay and the QKD backbone node. Hence, the required number of LKMs for a QKD chain request r can be formulated as

$$\alpha_{\mathrm{KM}}^{r} = \sum_{(i,j)\in L_r} \left\lceil \frac{l_{(i,j)}}{D} + 1 \right\rceil \tag{8}$$

We assume that the LKM is not shared by different QKD chain requests, since the QKD chains are independent of each other and may be run by different operators. Specifically, the LKM is a device/module with limited ports and capacity [53], [59], such that it can only be connected to a limited number of MDI-QTxs and store a limited amount of secret keys. From the networking perspective, it is possible that different QKD chains own the same secret-key rate. This is because the LKM can store and manage the local secret keys generated on each chain segment, and balance the achievable secret-key rate of the entire QKD chain. Based on (8), the cost of LKMs for all QKD chain requests can be formulated as

$$C_{\mathrm{KM}}^{R} = \sum_{r\in R} \gamma_{\mathrm{KM}}^{r} \cdot \alpha_{\mathrm{KM}}^{r} \tag{9}$$

where γ_{KM}^{r} is the cost of an LKM for the QKD chain request r.

3) Cost of GKSs: A GKS is required only in each QKD backbone node during the deployment phase, such that the required number of GKSs is independent of the number of QKD chain requests. The cost of GKSs is not considered in this study owing to its fixed and relatively low value.

4) Cost of SIs: SIs are required to protect both trusted relays and QKD backbone nodes. The required number of trusted relays for a QKD chain request r can be formulated as

$$\alpha_{\mathrm{TR}}^{r} = \sum_{(i,j)\in L_r} \left\lceil \frac{l_{(i,j)}}{D} - 1 \right\rceil \tag{10}$$

Considering that a QKD backbone node is usually operated with the safeguard on duty, the cost of the SI for a QKD backbone node is mainly associated with the operation cost so that it is not considered in the deployment phase. Hence, the cost of SIs for all QKD chain requests can be formulated as

$$C_{\mathrm{SI}}^{R} = \sum_{r\in R} \gamma_{\mathrm{SI}}^{r} \cdot \alpha_{\mathrm{TR}}^{r} \tag{11}$$

where γ_{SI}^{r} is the cost of the SI for a trusted relay of the QKD chain request r.

5) Cost of MUX/DEMUX Components: In order to enable the coexistence of QKD, KM, and optical links in the same fiber, MUX/DEMUX components are required at the physical location of each QKD/relay node (i.e., QKD backbone node, trusted relay, and untrusted relay). As described above, we assume that a trusted relay or an untrusted relay is deployed at the same physical location as an EDFA. The MUX/DEMUX components in optical backbone nodes can be reused for QKD backbone nodes for coexistence purposes. Accordingly, the required number of MUX/DEMUX component pairs for a QKD chain request r can be formulated as

$$\alpha_{\mathrm{MD}}^{r} = \sum_{(i,j)\in L_r} \left\lceil \frac{l_{(i,j)}}{D} \right\rceil + \sum_{(i,j)\in L_r} \left\lceil \frac{l_{(i,j)}}{D} - 1 \right\rceil \tag{12}$$

where the former and latter terms represent the required numbers of MUX/DEMUX component pairs in the untrusted and trusted relays, respectively. To maintain the stability and isolation of each QKD chain, we assume that different QKD chain requests cannot share their individual MUX/DEMUX components. The stability means the low impact is caused by channel perturbations on the performance (e.g., secret-key rate) of different QKD chains. The isolation is to avoid resource conflicts (e.g., the quantum channels of different QKD chains competing for the same wavelength) when different QKD chains are run by different operators. Based on (12), the cost of MUX/DEMUX components for all QKD chain requests can be formulated as

$$C_{\mathrm{MD}}^{R} = \sum_{r\in R} \gamma_{\mathrm{MD}}^{r} \cdot \alpha_{\mathrm{MD}}^{r} \tag{13}$$

where γ_{MD}^{r} is the cost of a pair of MUX/DEMUX components for the QKD chain request r.

6) Cost of QKD and KM Links: As described in Section III, we assume that a QKD link occupies three wavelength channels (i.e., one wavelength channel for transmitting quantum signals and two wavelength channels for synchronization, distillation and other functions by exchanging classical signals [53]) and a KM link occupies one wavelength channel [25] in this study. An optical link includes high-speed data channels that usually occupy a number of wavelength channels at C-band (1530–1565 nm). The quantum channel can be placed at both C-band and O-band (1260–1360 nm) to coexist with the classical channels in the same fiber. To achieve better channel isolation (i.e., large quantum-classical channel separation at the level of THz), the quantum channel is placed at O-band in this study. Such a channel allocation plan has been validated in the field trials of QKD-integrated optical backbone networks [25], [60]. In this work, each wavelength channel in different fibers is fairly allocated. Additionally, we assume that different QKD chains cannot share the same fiber in order to enhance stability and isolation. All quantum channels (for QKD links)

and classical channels (for QKD and KM links) required by a QKD chain, as well as high-speed data channels (for optical links) required for classical optical communications, are multiplexed in the same fiber of the existing optical backbone network. The physical length of QKD and KM links for a QKD chain request r can be formulated as

$$l^r_{\mathrm{Ch}} = \sum_{(i,j)\in L_r} \left(3 \cdot \eta_r \cdot l_{(i,j)} + l_{(i,j)}\right) \tag{14}$$

where the former and latter terms represent the physical lengths of QKD links and KM links, respectively. Based on (14), the cost of links for all QKD chain requests can be formulated as

$$C^R_{\mathrm{Ch}} = \sum_{r\in R} \gamma^r_{\mathrm{Ch}} \cdot l^r_{\mathrm{Ch}} \tag{15}$$

where γ^r_{Ch} is the cost per kilometer of a wavelength channel on a fiber link for the QKD chain request r. Notably, the cost of different wavelength channels in a single fiber is assumed to be the same. The indicated cost per wavelength channel applies only external to the fiber infrastructure owner, such as QKD network operators buying bandwidth from a telecom provider. The number of wavelength channels available to QKD network operators relies on the number of wavelengths offered by the fiber infrastructure owner.

7) Total Deployment Cost: The total cost of deploying QKD with hybrid trusted/untrusted relays over an existing optical backbone network can be formulated as

$$C^R_{\mathrm{Total}} = C^R_{\mathrm{Tx}} + C^R_{\mathrm{Rx}} + C^R_{\mathrm{KM}} + C^R_{\mathrm{SI}} + C^R_{\mathrm{MD}} + C^R_{\mathrm{Ch}} \tag{16}$$

where the six terms can be computed based on the (6), (7), (9), (11), (13), and (15), respectively. Some potential auxiliary equipment (e.g., optical switch and additional fibers) may also be installed during the network deployment phase, which are ignored in this study because their costs account for a very small part of the total deployment cost. It is important to note that the cost values of various network components may be fixed or flexible for QKD chain requests in different cases, which will be discussed in Section VII.

C. Security Model

As discussed in Sections I and III, the security level of a QKD backbone network becomes lower as the number of trusted relays for QKD chain requests increases. The reason is that the trusted relays constitute weak points of security in practice. Accordingly, we define the security level of a QKD backbone network as the ratio of 1 to the average number of trusted relays for each QKD chain request, which can be expressed as

$$SL_R = \frac{1}{\alpha^R_{\mathrm{TR}}/|R|} = \frac{|R|}{\alpha^R_{\mathrm{TR}}} = \frac{|R|}{\sum_{r\in R}\alpha^r_{\mathrm{TR}}} \tag{17}$$

where α^R_{TR} is the total number of trusted relays for all QKD chain requests. Notably, the security level is not the objective considered in this work, but the measure to understand the security of the resulted design.

V. Integer Linear Programming Model

Based on above network and cost models, in this section, we present an ILP model to conduct the cost optimization for deploying QKD with hybrid trusted/untrusted relays over an optical backbone network. According to the parameters and variables defined in Table II, the objective and constraints of this ILP model are described below.

The objective of the presented ILP model is to minimize the total deployment cost defined in (16), which can be formulated as

$$\text{Minimize } C^R_{\mathrm{Total}} = C^R_{\mathrm{Tx}} + C^R_{\mathrm{Rx}} + C^R_{\mathrm{KM}} + C^R_{\mathrm{SI}} + C^R_{\mathrm{MD}} + C^R_{\mathrm{Ch}} \tag{18}$$

where each term can be computed as follows:

$$C^R_{\mathrm{Tx}} = \sum_{r\in R}\sum_{(i,j)\in L}\sum_{\lambda\in W_{\mathrm{Q}}} \gamma^r_{\mathrm{Tx}} \cdot \frac{2\cdot f^r_{(i,j),\lambda}}{3} \cdot \left\lceil \frac{l_{(i,j)}}{D} \right\rceil \tag{19}$$

$$C^R_{\mathrm{Rx}} = \sum_{r\in R}\sum_{(i,j)\in L}\sum_{\lambda\in W_{\mathrm{Q}}} \gamma^r_{\mathrm{Rx}} \cdot \frac{f^r_{(i,j),\lambda}}{3} \cdot \left\lceil \frac{l_{(i,j)}}{D} \right\rceil \tag{20}$$

$$C^R_{\mathrm{KM}} = \sum_{r\in R}\sum_{(i,j)\in L}\sum_{w\in W_{\mathrm{M}}} \gamma^r_{\mathrm{KM}} \cdot x^r_{(i,j),w} \cdot \left\lceil \frac{l_{(i,j)}}{D} + 1 \right\rceil \tag{21}$$

$$C^R_{\mathrm{SI}} = \sum_{r\in R}\sum_{(i,j)\in L}\sum_{w\in W_{\mathrm{M}}} \gamma^r_{\mathrm{SI}} \cdot x^r_{(i,j),w} \cdot \left\lceil \frac{l_{(i,j)}}{D} - 1 \right\rceil \tag{22}$$

$$C^R_{\mathrm{MD}} = \sum_{r\in R}\sum_{(i,j)\in L}\sum_{w\in W_{\mathrm{M}}} \gamma^r_{\mathrm{MD}} \cdot x^r_{(i,j),w} \cdot \left(\left\lceil \frac{l_{(i,j)}}{D} \right\rceil + \left\lceil \frac{l_{(i,j)}}{D} - 1 \right\rceil\right) \tag{23}$$

$$C^R_{\mathrm{Ch}} = \sum_{r\in R}\sum_{(i,j)\in L}\sum_{\lambda\in W_{\mathrm{Q}}}\sum_{w\in W_{\mathrm{M}}} \gamma^r_{\mathrm{Ch}} \cdot \left(f^r_{(i,j),\lambda}\cdot l_{(i,j)} + x^r_{(i,j),w}\cdot l_{(i,j)}\right) \tag{24}$$

This objective must be subject to the following constraints:

$$\sum_{j\in N}\sum_{\lambda\in W_{\mathrm{Q}}}\sum_{w\in W_{\mathrm{M}}} \left(f^r_{(i,j),\lambda} + x^r_{(i,j),w}\right) - \sum_{j\in N}\sum_{\lambda\in W_{\mathrm{Q}}}\sum_{w\in W_{\mathrm{M}}} \left(f^r_{(j,i),\lambda} + x^r_{(j,i),w}\right) = \begin{cases} 3\cdot\eta_r + 1 & i = s_r \\ -3\cdot\eta_r - 1 & i = d_r \\ 0 & \text{else} \end{cases} \quad \forall r \in R \tag{25}$$

$$\sum_{\lambda\in W_{\mathrm{Q}}} f^r_{(i,j),\lambda} = 3\cdot\eta_r \cdot \sum_{w\in W_{\mathrm{M}}} x^r_{(i,j),w} \quad \forall r\in R, (i,j)\in L \tag{26}$$

$$\sum_{j\in N} f^r_{(i,j),\lambda} = \sum_{j\in N} f^r_{(j,i),\lambda} \quad \forall r \in R, i \in N, i \neq s_r, i \neq d_r, \lambda \in W_{\mathrm{Q}} \tag{27}$$

$$\sum_{j\in N} x^r_{(i,j),w} = \sum_{j\in N} x^r_{(j,i),w} \quad \forall r \in R, i \in N, i \neq s_r, i \neq d_r, w \in W_{\mathrm{M}} \tag{28}$$

$$\sum_{r\in R}\sum_{\lambda\in W_{\mathrm{Q}}} f^r_{(i,j),\lambda} \leq |W_{\mathrm{Q}}| \quad \forall (i,j) \in L \tag{29}$$

$$\sum_{r\in R}\sum_{w\in W_{\mathrm{M}}} x^r_{(i,j),w} \leq |W_{\mathrm{M}}| \quad \forall (i,j) \in L \tag{30}$$

$$\sum_{r\in R} f^r_{(i,j),\lambda} \leq 1 \quad \forall (i,j) \in L, \lambda \in W_{\mathrm{Q}} \tag{31}$$

$$\sum_{r\in R} x^r_{(i,j),w} \leq 1 \quad \forall (i,j) \in L, w \in W_{\mathrm{M}} \tag{32}$$

Equation (25) is the flow conservation constraint. Equation (26) specifies the number of wavelength channels required by the QKD and KM links of each QKD chain request, where the QKD and KM links need to occupy $3\eta_r$ and 1 wavelength channels, respectively. Equations (25) and (26) ensure that only one path is selected between the source and destination QKD backbone nodes of each QKD chain request, in which the QKD link and the KM link of each QKD chain request are on the same path. Equations (27) and (28) are wavelength continuity constraints ensuring that the same wavelength channels for the QKD/KM links are assigned along the selected path for each QKD chain request. Equations (29) and (30) ensure that the wavelength channels for the QKD/KM links of all QKD chain requests should be no more than the total number of available wavelength channels. Equations (31) and (32) are wavelength uniqueness constraints ensuring that any wavelength channel for the QKD/KM link can only be assigned once.

The complexity of the ILP formulation generally depends on the dominant numbers of variables and constraints. In the proposed ILP model, the dominant number of variables is $O(|R||L||W_{\mathrm{Q}} \cup W_{\mathrm{M}}|)$, and the dominant number of constraints is $O(|R||L| + |W_{\mathrm{Q}} \cup W_{\mathrm{M}}|(|R||N| + |L|))$.

VI. Heuristic Algorithm Design

The presented ILP model provides an optimal solution to minimize the total deployment cost. However, it is not scalable for large-scale networks owing to its high computational complexity. Therefore, in this section, we present a heuristic algorithm to obtain a fast solution to cost optimization for QKD backbone network deployment.

According to the notations listed in Table II, Algorithm 1 shows the detailed procedure of the presented cost-optimized QKD backbone networking (CO-QBN) algorithm. Lines 1 and 5 are for the initialization. The for-loop covering lines 2–35 accomplishes the CO-QBN by processing all QKD chain requests, in which lines 3–34 are processed for each QKD chain request in R. For a QKD chain request, K *shortest paths*

Algorithm 1: CO-QBN Algorithm

Input: $G(N, L)$, $l_{(i,j)}$, W_{Q}, W_{M}, τ, R, γ^r_{Tx}, γ^r_{Rx}, γ^r_{KM}, γ^r_{SI}, γ^r_{MD}, γ^r_{Ch}.

Output: α^R_{TR}, C^R_{Total}, routing and channel allocation for each QKD chain request, updated network status.

1 initialize $\alpha^R_{\mathrm{TR}} \leftarrow 0$, $C^R_{\mathrm{Total}} \leftarrow 0$;
2 **for** *each QKD chain request* $r \in R$ **do**
3 routing computation with K*-shortest-path* algorithm;
4 **for** *each alternative path* p_r **do**
5 initialize α^r_{Tx}, α^r_{Rx}, α^r_{KM}, α^r_{TR}, α^r_{MD}, $l^r_{\mathrm{Ch}} \leftarrow 0$;
6 find all fiber links on p_r and insert them into set $L(p_r)$;
7 find available wavelength channels in W_{Q} on p_r and insert them into set $W_{\mathrm{Q}}(p_r)$;
8 **if** $|W_{\mathrm{Q}}(p_r)| \geq 3\eta_r$ **then**
9 find available wavelength channels in W_{M} on p_r and insert them into set $W_{\mathrm{M}}(p_r)$;
10 **if** $|W_{\mathrm{M}}(p_r)| \geq 1$ **then**
11 select $3\eta_r$ wavelength channels from $W_{\mathrm{Q}}(p_r)$ with *first-fit* algorithm for the QKD link of r;
12 select one wavelength channel from $W_{\mathrm{M}}(p_r)$ with *first-fit* algorithm for the KM link of r;
13 **for** *each fiber link* $e \in L(p_r)$ **do**
14 obtain the physical length $l_{(i,j)}$ of e;
15 $\alpha^r_{\mathrm{Tx}} \leftarrow \alpha^r_{\mathrm{Tx}} + 2 \cdot \eta_r \cdot \lceil l_{(i,j)}/D \rceil$;
16 $\alpha^r_{\mathrm{Rx}} \leftarrow \alpha^r_{\mathrm{Rx}} + \eta_r \cdot \lceil l_{(i,j)}/D \rceil$;
17 $\alpha^r_{\mathrm{KM}} \leftarrow \alpha^r_{\mathrm{KM}} + \lceil l_{(i,j)}/D + 1 \rceil$;
18 $\alpha^r_{\mathrm{TR}} \leftarrow \alpha^r_{\mathrm{TR}} + \lceil l_{(i,j)}/D - 1 \rceil$;
19 $\alpha^r_{\mathrm{MD}} \leftarrow \alpha^r_{\mathrm{MD}} + \lceil l_{(i,j)}/D \rceil + \lceil l_{(i,j)}/D - 1 \rceil$;
20 $l^r_{\mathrm{Ch}} \leftarrow l^r_{\mathrm{Ch}} + 3 \cdot \eta_r \cdot l_{(i,j)} + l_{(i,j)}$;
21 **end**
22 $C^r_{\mathrm{Total}} \leftarrow \gamma^r_{\mathrm{Tx}} \cdot \alpha^r_{\mathrm{Tx}} + \gamma^r_{\mathrm{Rx}} \cdot \alpha^r_{\mathrm{Rx}} + \gamma^r_{\mathrm{KM}} \cdot \alpha^r_{\mathrm{KM}} + \gamma^r_{\mathrm{SI}} \cdot \alpha^r_{\mathrm{TR}} + \gamma^r_{\mathrm{MD}} \cdot \alpha^r_{\mathrm{MD}} + \gamma^r_{\mathrm{Ch}} \cdot l^r_{\mathrm{Ch}}$;
23 record C^r_{Total} and α^r_{TR} for p_r;
24 **else**
25 **continue**;
26 **end**
27 **else**
28 **continue**;
29 **end**
30 **end**
31 select the path p_r with minimum C^r_{Total} for r;
32 $C^R_{\mathrm{Total}} \leftarrow C^R_{\mathrm{Total}} + C^r_{\mathrm{Total}}$;
33 $\alpha^R_{\mathrm{TR}} \leftarrow \alpha^R_{\mathrm{TR}} + \alpha^r_{\mathrm{TR}}$;
34 update network status;
35 **end**
36 **return** α^R_{TR}, C^R_{Total}, routing and channel allocation for each QKD chain request, updated network status.

between its source and destination QKD backbone nodes are computed using *K-shortest-path* algorithm (line 3). In the *K-shortest-path* algorithm, *K shortest paths* between the source and destination nodes are computed in order and selected as the alternative paths.

In order to select the optimal path from alternative paths, the inner for-loop that covers lines 4–30 computes the deployment cost for each alternative path of the QKD chain request. Line 6 finds all fiber links on the alternative path. Lines 7–10 check whether the available wavelength channels on the alternative path can satisfy the wavelength requirements of the QKD chain request, where the wavelength continuity is considered. If the wavelength requirements can be satisfied, the *first-fit* algorithm is utilized for wavelength channel allocation to the QKD link (line 11) and the KM link (line 12). Otherwise the next alternative path will be checked. In the *first-fit* algorithm, all the available wavelength channels are numbered and an available wavelength channel with the smallest serial number is selected. The *first-fit* algorithm is simple but efficient, which is widely used for resource allocation [35], [40], [46].

The inner for-loop that covers lines 13–21 computes the required numbers of various components as well as the physical length of links for the alternative path of the QKD chain request. The deployment cost for the alternative path of QKD chain request is computed (line 22) and recorded (line 23). In line 31, the alternative path with the minimum deployment cost is selected as the optimal path for QKD chain request. Lines 32–33 perform further computations, with the ultimate goal of computing the total deployment cost and the total number of trusted relays for all QKD chain requests.

In the worst case, the time complexities to process one QKD chain request in lines 3 and 4–34 are $O(K|N|(|L| + |N|\log|N|))$ and $O(K(|W_{\mathrm{Q}} \cup W_{\mathrm{M}}| + |N|))$, respectively. Consequently, the overall time complexity of the CO-QBN algorithm for processing one QKD chain request is $O(K(|N|(|L| + |N|\log|N|) + |W_{\mathrm{Q}} \cup W_{\mathrm{M}}|))$.

VII. Performance Evaluation and Analysis

In this section, we perform extensive simulations to evaluate the presented ILP model and heuristic algorithm. Given that the cost optimization for the deployment of QKD with hybrid trusted/untrusted relays has not been addressed before, a simple benchmark algorithm (called RANDOM algorithm hereinafter) is utilized for comparison, which realizes random routing (i.e., random path selection from all possible paths between the source and destination nodes) and random channel allocation for each QKD chain request. The RANDOM algorithm is used to represent an upper bound on the overall cost, since the ILP model and CO-QBN algorithm are designed to optimize the overall cost. The random-path routing used in the RANDOM algorithm is a common routing method used in QKD networks [61], [62], where the randomness of routing can enhance the network resilience against various failures (e.g., link failures). Moreover, we conduct a comparative analysis of the hybrid trusted/untrusted relay and purely trusted relay schemes in terms of deployment cost, network component usage, and security level.

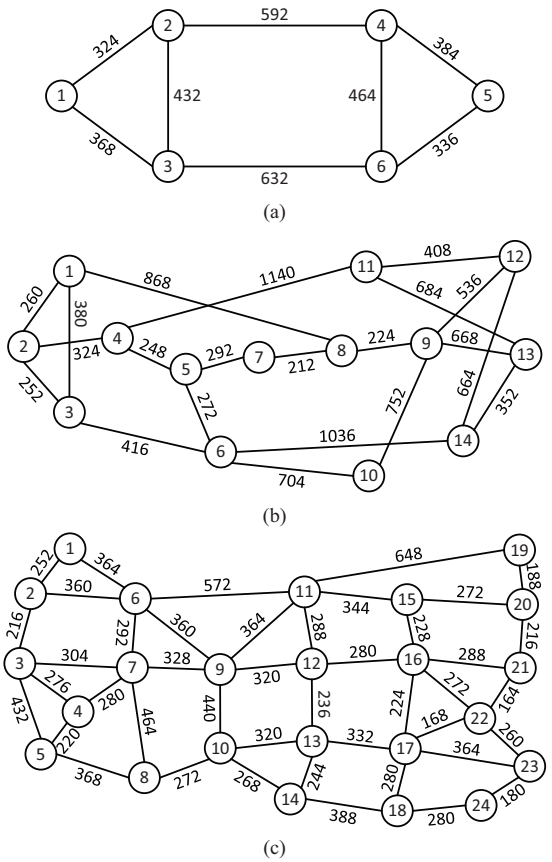


Fig. 4. Network topologies used in simulations: (a) six-node network topology; (b) NSFNET topology; (c) USNET topology.

As shown in Fig. 4, three backbone network topologies are utilized in simulations. A six-node small network topology in Fig. 4(a) is adopted to compare the performance of the ILP model and heuristics for verifying the effectiveness of the presented CO-QBN algorithm. Further, two large network topologies, i.e., 14-node NSFNET topology in Fig. 4(b) and 24-node USNET topology in Fig. 4(c), are adopted for the detailed deployment cost and security level analysis. The physical length (in km) of each fiber link is marked on the network topologies. We assume that the available wavelength channels on each fiber link are sufficient, such that each QKD chain request can be successfully accommodated over the existing optical backbone network. The distance between a QKD transmitter (QTx) and its connected QKD receiver (QRx) is $\sim$80 km, that is, each trusted/untrusted relay is placed in the same physical location as an EDFA. In addition, each QKD chain request is randomly generated between any two QKD backbone nodes, and K is configured to 3 in the *K-shortest-path* algorithm to provide three alternative paths for each QKD chain request.

The simulations run on a computer with 2.5 GHz Intel Core i5-7200U CPU and 8 GB RAM. The ILOG CPLEX V12.2 and IntelliJ IDEA 2017 are installed in this computer to solve the ILP model and implement the heuristics, respectively. In order to maintain sufficient statistical accuracy, the simulation results are averaged with 100 times repetition.

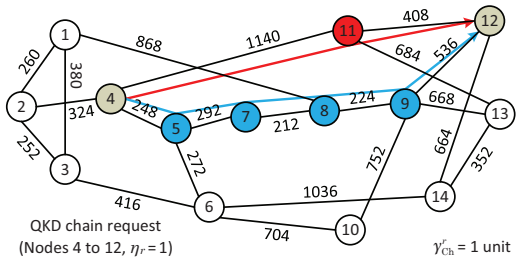
TABLE III
COST VALUES USED FOR PERFORMANCE EVALUATION AND ANALYSIS

QKD backbone network	Case	$\|R\|$	γ^r_{Tx}(units)	γ^r_{Rx}(units)	γ^r_{KM}(units)	γ^r_{SI}(units)	γ^r_{MD}(units)	γ^r_{Ch}(units)
Hybrid trusted/untrusted relay	SC	>0	1500	2250	1200	150	300	[1, 2]
	UC	>0	[1000, 1500]	[1500, 2250]	[800, 1200]	[100, 150]	[200, 300]	[1, 2]
	DC	$(0, 0.5\rho]$	1500	2250	1200	150	300	[1, 2]
		$(0.5\rho, \rho]$	1250	1875	1000	125	250	[1, 2]
		$>\rho$	1000	1500	800	100	200	[1, 2]
Purely trusted relay	SC	>0	1500	2250	1200	150	300	[1, 2]

In particular, the total cost of QKD backbone network deployment is highly dependent on the costs of various network components (including devices and links). Considering the maturity of the technology and the sales volume, the costs of devices usually have a large degree of uncertainty. As an example, the cost of QKD transceivers can be reduced in the future by using chip-scale integrated photonic devices [63], [64]. However, the cost of links can maintain relatively stable over a long period of time, since fiber links have been installed in the existing optical backbone networks.

In this study, we consider the following three cases: 1) a static case (SC) where the cost values of devices are fixed over the time and independent of the quantity of the QKD chain requests; 2) a uniform case (UC) where the cost values of devices are uniformly distributed within a certain range, meaning that some QKD chain requests come later and cost less to be deployed; 3) a dynamic case (DC) where the cost values of devices depend on the number of QKD chain requests, i.e., the cost is reduced when the number of QKD chain requests increases. The SC with fixed cost values is mainly suitable for the network to be deployed in a short term, where the device cost is relatively stable. The UC and DC with flexible cost values can be used for the network deployment and upgrade carried out gradually over the entire network lifetime. Due to mature of techniques and massive deployment in future, the device cost is expected to be reduced. Both the UC and DC consider that the device cost will decrease by time, which is helpful to evaluate the impact of our cost optimization in a long run.

The cost values used for performance evaluation and analysis are listed in Table III, where the unit represents a normalized cost unit. Since there are no officially disclosed cost values of devices required in the QKD backbone network, the cost values of devices in Table III are relative to the cost value of links and are assumed based on some practical systems/networks. We assume that the cost value of links (i.e., γ^r_{Ch}) is uniformly distributed within [1, 2] units in three cases. The parameter $|R|$ in Table III represents the total number of QKD chain requests. When the value of $|R|$ is larger than zero, the device costs are fixed in the SC, and the device costs are uniformly distributed within a certain range in the UC. In the DC, three intervals are considered for the value of $|R|$, namely $(0, 0.5\rho]$, $(0.5\rho, \rho]$, and $(\rho, +\infty)$. These three intervals represent the incremental QKD chain requests, where the device costs are reduced with the growing number of QKD chain requests due to the increased sales volume.



Path	α^r_{Tx}	α^r_{Rx}	α^r_{KM}	α^r_{TR}	α^r_{MD}	l^r_{Ch}	Deployment cost in SC
Blue path (Shortest)	24	12	17	7	19	6048 km	96198 units
Red path (CO-QBN)	22	11	13	9	20	6192 km	86892 units

Fig. 5. A counterexample showing that the shortest path is not always the optimal solution.

For a fair comparison, we also introduce the purely trusted relay based QKD deployment over optical backbone networks. The results are computed using a variant of the CO-QBN algorithm according to the cost-oriented formulations for a purely trusted relay based QKD backbone network in [50]. We use a variant of the CO-QBN algorithm rather than the existing heuristic algorithm, such as [50], for two reasons: 1) the device types considered are not the same as those considered in the existing work; 2) the direct use of the existing heuristic algorithm, e.g., [50], could result in an unfair comparison since different routing methods are adopted. In addition, the same cost assumptions are used for MDI-QKD and conventional point-to-point QKD in the SC to ensure a fair comparison of the hybrid trusted/untrusted relay and purely trusted relay schemes. Accordingly, the parameters γ^r_{Tx} and γ^r_{Rx} represent the costs of a QTx and a QRx based on conventional point-to-point QKD protocols (e.g., BB84, COW, and GG02) in the SC for a purely trusted relay based QKD backbone network, respectively.

Moreover, to make the distinction between the problem addressed in this paper and the optimization problem aiming at shortest-path routing more evident, we give a counterexample to show that the shortest path is not always the optimal solution for the problem addressed in this paper. As illustrated in Fig. 5, the shortest path for a QKD chain request ($\eta_r = 1$) from Node 4 to Node 12 is the blue path (passing through Nodes 5, 7, 8, and 9). The path selected for this QKD chain request using

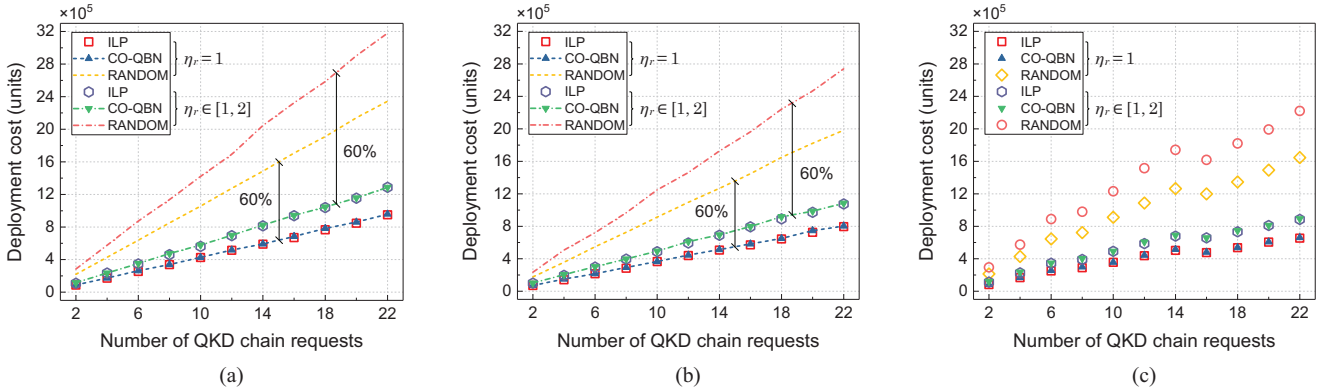


Fig. 6. Deployment cost of QKD with hybrid trusted/untrusted relays versus number of QKD chain requests on the six-node network topology: (a) SC; (b) UC; (c) DC.

the CO-QBN algorithm is the red path (passing through Node 11). The required numbers of various components and the deployment costs for the two paths of this QKD chain request are compared in Fig. 5. The red path has lower deployment cost but is longer than the blue one.

A. CO-QBN Algorithm Verification

The six-node network topology (ρ = 15) is adopted for CO-QBN algorithm verification. We set the number of QKD chain requests within [2, 22]. The deployment cost of QKD with hybrid trusted/untrusted relays versus number of QKD chain requests is illustrated in Fig. 6. Three cases, i.e., SC, UC, and DC, are depicted in Figs. 6(a), 6(b), and 6(c), respectively. We consider different secret-key rate requirements, covering the fixed value of $\eta_r = 1$ and the flexible value of $\eta_r \in [1, 2]$ for each QKD chain request. In addition to the results for the ILP model and the CO-QBN algorithm, we include the results for the RANDOM algorithm for performance comparison.

From Figs. 6(a) and 6(b) we can see the deployment cost grows linearly as the number of QKD chain requests increases. While in Fig. 6(c), the deployment cost increases linearly with the number of QKD chain requests in [2, 6], [8, 14], and [16, 22], respectively. Such a linear tendency stems from the random generation of QKD chain requests between any two QKD backbone nodes. The increase in deployment cost is due to the increase in network components required to accommodate more QKD chain requests. The reason for the special variation tendency of the deployment cost shown in Fig. 6(c) is that the cost values of various devices change dynamically with the number of QKD chain requests, and hence discrete points are plotted in the DC. It can also be observed that the deployment cost under $\eta_r \in [1, 2]$ is larger than that under $\eta_r = 1$. This is because more network components need to be deployed to fulfil the increased secret-key rate requirements of some QKD chain requests.

In different cases (SC/UC/DC) with the fixed/flexible values of η_r, the deployment cost with the presented ILP model or CO-QBN algorithm is much lower than that with the RANDOM algorithm. This phenomenon indicates that the presented approaches have the advantages of achieving the cost optimization to deploy QKD over existing optical backbone networks and being applicable for a long run. The cost savings of the presented approaches relative to the benchmark algorithm are ∼60% and basically remain stable with the variation of η_r. It reflects that the cost saving is weakly related to the secret-key rate requirement. In particular, the CO-QBN algorithm performs very similar to the ILP model under different circumstances, demonstrating its near-optimal characteristic. Although this near-optimal characteristic is affected by the physical lengths of fiber links and the assumption that sufficient wavelength resources are available, the presented CO-QBN algorithm is still an effective approach to achieve cost optimization for QKD deployment over optical backbone networks. Additionally, by comparing the results of RANDOM and CO-QBN algorithms, we can deduce that the randomness of routing enhances the survivability but sacrifices the deployment cost. This reflects a trade-off between deployment cost and survivability.

The running time is less than one second for the CO-QBN algorithm, whereas it can reach a few hundreds of seconds for the ILP model. For example, when the number of QKD chain requests is 22, the running time for the ILP model and CO-QBN algorithm are 228 seconds and 0.213 seconds in the SC, respectively. Hence, the CO-QBN algorithm is much more time-efficient than the ILP model. Given that the ILP model becomes intractable when the number of QKD chain requests and the network size become larger, the deployment cost, network component usage, and security level analysis on the large network topologies in subsequent subsections will adopt the CO-QBN algorithm.

B. Deployment Cost Analysis

The NSFNET topology (ρ = 91) and USNET topology (ρ = 276) are utilized for further deployment cost analysis. We set the number of QKD chain requests within [15, 165] and [35, 385] on NSFNET and USNET topologies, respectively. The fixed value of $\eta_r = 1$ is considered for each QKD chain request.

The deployment cost of QKD with hybrid trusted/untrusted relays versus number of QKD chain requests is shown in Fig. 7, where three cases are considered for both CO-QBN and RANDOM algorithms. For comparison purpose, we also

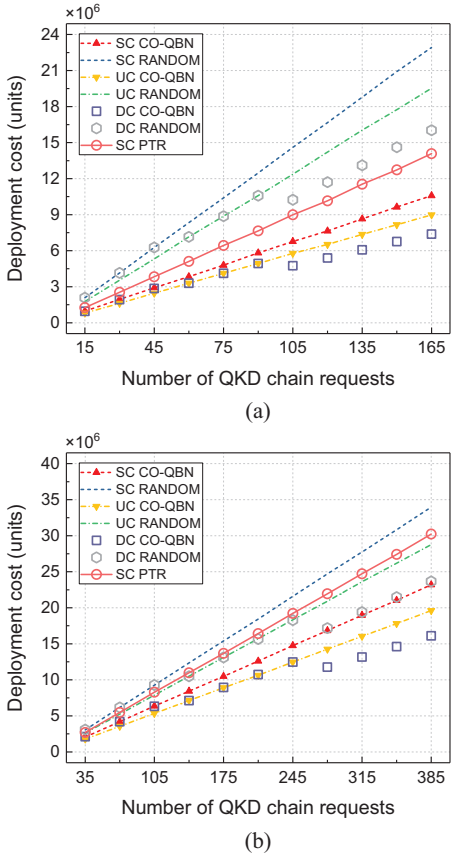


Fig. 7. Deployment costs of QKD with hybrid trusted/untrusted relays (SC/UC/DC CO-QBN/RANDOM) and purely trusted relays (SC PTR) versus number of QKD chain requests: (a) NSFNET topology; (b) USNET topology.

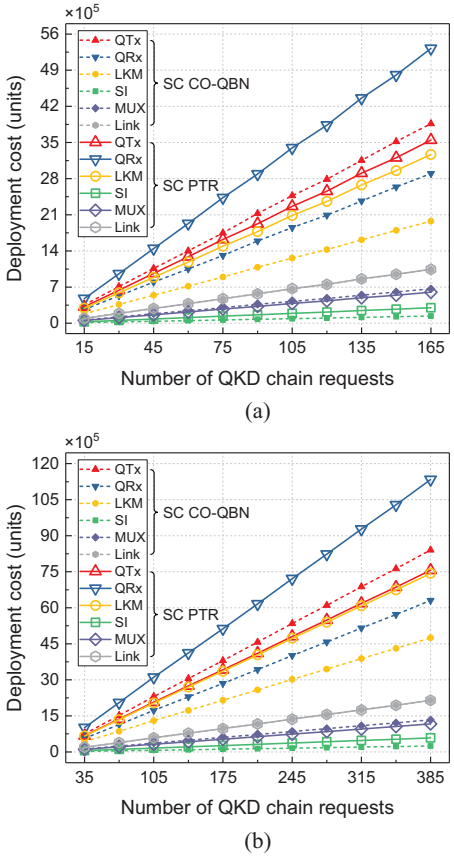


Fig. 8. Deployment costs of various network components in the hybrid trusted/untrusted relay and purely trusted relay schemes versus number of QKD chain requests: (a) NSFNET topology; (b) USNET topology. (Link covers QKD and KM links, MUX represents MUX/DEMUX components)

include the results (SC PTR in Fig. 7) for deploying QKD with purely trusted relays. It can be observed that the results in SC/UC show the linear tendency with the growing QKD chain requests on different backbone network topologies. While in the DC, the results first demonstrate similarly to that in the SC, then perform similarly to that in the UC, and increase linearly with the number of QKD chain requests in [105, 165] and [280, 385] on NSFNET and USNET topologies, respectively. These phenomena have been explained in the previous subsection. In the DC, the device costs change when the number of QKD chain requests is higher than a certain number.

As illustrated in Figs. 7(a) and 7(b), the results in each case with the CO-QBN algorithm are much lower than that with the RANDOM algorithm on NSFNET and USNET topologies. Hence, the applicability of the presented CO-QBN algorithm in different network topologies for a long run is verified. Specifically, in the SC, the deployment cost (SC CO-QBN in Fig. 7) of QKD with hybrid trusted/untrusted relays is lower than that (SC PTR in Fig. 7) with purely trusted relays. This can be explainable by analyzing the cost distribution of various network components during the deployment phase, which will be detailed in the following paragraphs. Note that the QTx and QRx based on conventional point-to-point QKD protocols (e.g., BB84, COW, and GG02) are cheaper than the MDI-QTx and MDI-QRx today. Nonetheless, the comparison results in Fig. 7 indicate that the total deployment cost can be significantly reduced when the MDI-QKD is technically more mature and its device costs can reach the level of conventional point-to-point QKD. Specifically, the experiment in [65] demonstrated that the MDI-QKD system can be reconfigured to be the conventional point-to-point QKD system, indicating that MDI-QKD has the potential to reach the level of conventional point-to-point QKD in terms of device costs. Moreover, chip-based QKD [63], [64] can further reduce the cost gap between MDI-QKD and conventional point-to-point QKD devices.

According to Fig. 7, the cost savings of CO-QBN versus RANDOM/PTR in different cases on NSFNET and USNET topologies are listed in Table IV. In each case, the cost saving basically keeps stable with the variation of the number of QKD chain requests. Specifically, the cost savings of the presented CO-QBN algorithm relative to the RANDOM algorithm can reach approximately 54% and 32% on NSFNET and USNET topologies, respectively. This phenomenon reflects that the cost saving of CO-QBN versus RANDOM is closely related to the network topology. When the network topology has lower node degrees, i.e., less connected, the *K-shortest-path* routing in the CO-QBN algorithm could significantly outperform the random routing in the RANDOM algorithm, leading to more cost savings. In addition, the deployment cost savings of the

TABLE IV
COST SAVINGS OF CO-QBN VERSUS RANDOM/PTR IN DIFFERENT CASES

NSFNET topology					USNET topology				
$\|R\|$	CO-QBN vs. RANDOM SC (%)	CO-QBN vs. RANDOM UC (%)	CO-QBN vs. RANDOM DC (%)	CO-QBN vs. PTR SC (%)	$\|R\|$	CO-QBN vs. RANDOM SC (%)	CO-QBN vs. RANDOM UC (%)	CO-QBN vs. RANDOM DC (%)	CO-QBN vs. PTR SC (%)
15	53.4	54.1	54.2	23.0	35	32.5	31.7	31.4	23.3
45	53.6	53.8	54.5	24.1	105	31.3	32.2	31.9	23.2
75	53.9	53.6	53.6	25.5	175	31.9	32.1	31.8	23.3
105	53.7	53.2	53.6	24.8	245	31.7	32.0	31.8	23.2
135	54.0	54.1	53.7	25.1	315	31.6	32.0	32.2	23.3
165	53.8	54.0	54.0	24.9	385	31.7	31.8	31.9	23.3

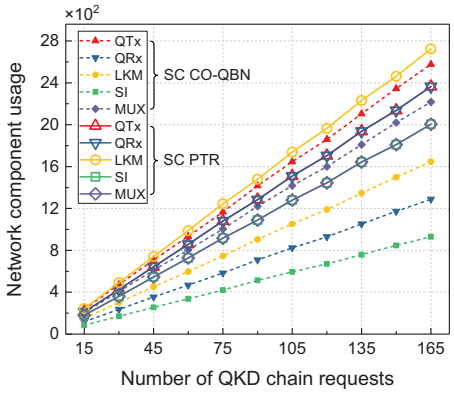
hybrid trusted/untrusted relay scheme relative to the purely trusted relay scheme are up to 25% and 23% on NSFNET and USNET topologies, respectively. Such a cost saving is weakly related to the network topology, thanks to the same routing algorithm employed for both relay schemes.

Based on the results (SC CO-QBN and SC PTR) in Fig. 7, the deployment costs of various network components in the hybrid trusted/untrusted relay and purely trusted relay schemes versus number of QKD chain requests are illustrated in Fig. 8. It can be observed that the deployment cost of QKD and KM links in the hybrid trusted/untrusted relay scheme is similar to that in the purely trusted relay scheme. This is because the same path is selected for a QKD chain request in both relay schemes. In addition, the deployment costs of QRx, LKM, and SI in the hybrid trusted/untrusted relay scheme are lower than those in the purely trusted relay scheme. The reason is that more QRxs and trusted relays are needed in the purely trusted relay scheme. However, the deployment costs of QTx and MUX/DEMUX components in the hybrid trusted/untrusted relay scheme are a little larger than those in the purely trusted relay scheme. This is due to the fact that QTx is deployed in a pair-wise manner in the hybrid trusted/untrusted relay scheme. For some QKD chain requests with specific lengths of QKD/KM links, e.g., the distance of the last chain segment for secret-key relay is less than τ ($\sim$80 km), such a pair-wise manner causes the total number of relays in the hybrid trusted/untrusted relay scheme to be a little larger than that in the purely trusted relay scheme.

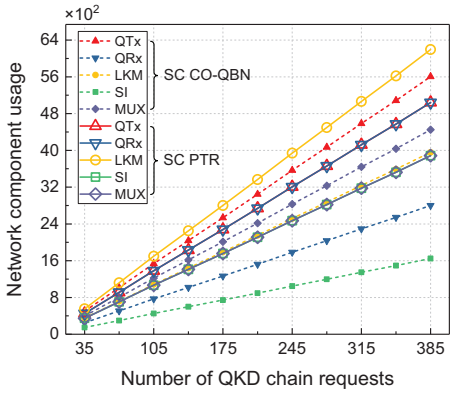
C. Network Component Usage Analysis

The network component usage (i.e., the required numbers of various network components) analysis is performed. This analysis does not depend on costs of the various components. The fixed value of $\eta_r = 1$ is considered for each QKD chain request, and the results are obtained based on SC CO-QBN and SC PTR. Figure 9 demonstrates the network component usage in the hybrid trusted/untrusted relay and purely trusted relay schemes versus number of QKD chain requests, in which the NSFNET and USNET topologies are adopted, but the physical lengths of QKD and KM links are not included. From Fig. 9 we can see that the network component usage increases linearly with the number of QKD chain requests, which can be attributed to the random generation of QKD chain requests.

In particular, we observe that the network component usage in a descending order is QTx $>$ MUX $>$ LKM $>$ QRx $>$ SI in the hybrid trusted/untrusted relay scheme, whereas it is LKM $>$ QTx = QRx $>$ SI = MUX in the purely trusted relay scheme. The demand for QRxs with the hybrid trusted/untrusted relay scheme is reduced compared to the purely trusted relay scheme. The reason is that in the hybrid scheme the MDI-QKD protocol allows two QTxs to be connected to one QRx, while in the purely trusted relay scheme the conventional point-to-point QKD protocols have a one-to-one relationship between



(a)



(b)

Fig. 9. Network component usage (i.e., the numbers of required network components) in the hybrid trusted/untrusted relay and purely trusted relay schemes versus number of QKD chain requests: (a) NSFNET topology; (b) USNET topology. (MUX represents MUX/DEMUX components)

QTx and QRx. It is obvious that the required numbers of QRxs, LKMs, and SIs can be significantly reduced when the hybrid trusted/untrusted relay scheme is adopted. Hence, if the QRxs, LKMs, and SIs own relatively high device costs, the hybrid trusted/untrusted relay scheme can achieve significant deployment cost savings compared to the purely trusted relay scheme. It should be noted that for QKD techniques, the cost of a QTx is often lower than that of a QRx. Moreover, novel sharing schemes designed to enable different QKD chain requests to share the MUX/DEMUX components or LKMs are beneficial to further reduce the total deployment cost.

D. Security Level Analysis

The security levels of the hybrid trusted/untrusted relay and the purely trusted relay based QKD backbone networks versus number of QKD chain requests are compared in Fig. 10, where the NSFNET and USNET topologies are considered, and the fixed value of $\eta_r = 1$ is utilized for each QKD chain request. From Figs. 10(a) and 10(b) we observe that the security level demonstrates approximately constant values with the growing number of QKD chain requests. This is because the average required number of trusted relays for each QKD chain request is the same. Also, the security level remains stable in different cases, since it is independent of different cost values according to (17).

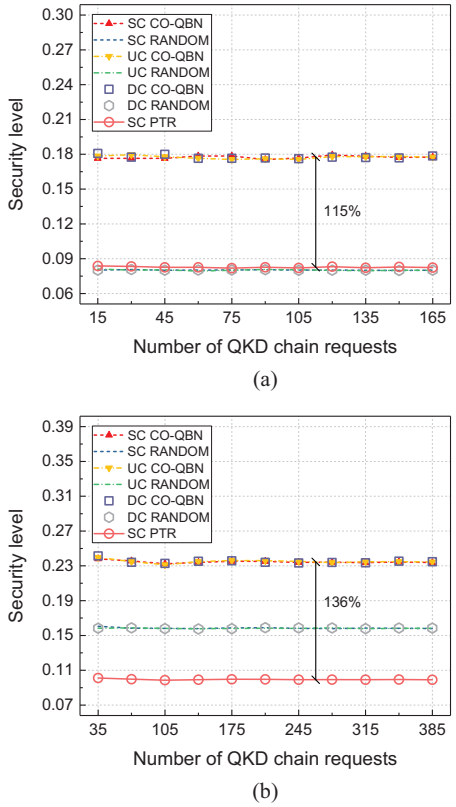


Fig. 10. Security levels of the hybrid trusted/untrusted relay (SC/UC/DC CO-QBN/RANDOM) and the purely trusted relay (SC PTR) based QKD backbone networks versus number of QKD chain requests: (a) NSFNET topology; (b) USNET topology.

The security level with the CO-QBN algorithm is higher than that with the RANDOM algorithm. Accordingly, the presented CO-QBN algorithm has the potential to achieve the optimal deployment of a hybrid trusted/untrusted relay based QKD backbone network, which can reduce the average required number of trusted relays for each QKD chain request. In addition, by comparing the results (SC CO-QBN and SC PTR), the security level enhancements of using the hybrid trusted/untrusted relay scheme versus the purely trusted relay scheme are up to 115% and 136% on NSFNET and USNET topologies, respectively. Consequently, deploying QKD based on the hybrid trusted/untrusted relay scheme can achieve a higher level of security than that based on the purely trusted relay scheme.

VIII. Open Issues

In this work, we make a first attempt to analyze the hybrid trusted/untrusted relay based QKD deployment over optical backbone networks. We strive to provide a more general consideration and explanation of various aspects in such a complex hybrid network architecture. Nonetheless, some assumptions are inevitably made in the models due to the limitations of technological development. We underline that our conclusions depend on assumptions regarding both the models and the crucial input (e.g., cost values). We expect that the system and network aspects of MDI-QKD integrated optical networks can develop synergistically and complement each other. Some issues listed below are still open and need to be addressed in future research.

1) MDI-QKD: The MDI-QKD protocol (2012) is invented later than the relatively mature BB84 (1984), COW (2005), and GG02 (2002) protocols. Some important directions, such as MDI-QKD over asymmetric channels and the coexistence of MDI-QKD with classical optical communications still require further investigations.

2) Flexible Location: The flexibility of QKD deployment over optical networks can be further enhanced. For example, a more flexible value of the physical distance between a pair of QKD devices can be considered under different constraints. Meanwhile, the flexible placement of hybrid trusted/untrusted relays will need to be studied.

3) Wavelength Limitation: The available wavelengths are assumed to be abundant in the performance evaluation. In the case of a limited number of wavelengths, the ILP model is able to accommodate more QKD chain requests than the heuristics and causes higher deployment cost. It does not mean the ILP model performs worse than the heuristics. Identifying new performance metrics could facilitate a fair comparison.

4) Fiber Type: Different types of fibers may have been installed in the existing optical backbone network, such that the cost values of wavelength channels in various types of fibers may be distinct. How to optimally assign the wavelength channels for multiple QKD chain requests becomes a future research challenge, where the physical-layer impairments and the total cost of ownership should be carefully evaluated.

5) Algorithm Optimization: The proposed CO-QBN algorithm is a basic algorithm with the objective to minimize the

deployment cost. Some algorithms with the modest additional complexity can be designed in the future to further optimize the network performance (not only the deployment cost, but also other performance metrics such as the security level).

6) Channel Allocation: This work is limited to the selected channel allocation scheme. On the other hand, many channel allocation schemes have been proposed and validated. The cost efficiency could be affected by various channel allocation schemes for QKD-integrated optical backbone networks, particularly when different QKD chain deployment strategies are implemented. The relevant performance evaluation and comparison should be carried out to gain an understanding of the impact of the channel allocation scheme on QKD-integrated optical backbone networks.

7) Network Operation: In addition to cost optimization for network deployment, many other aspects such as quality-of-service provisioning and cost optimization for network operation need to be investigated in the hybrid trusted/untrusted relay based QKD network.

8) Heterogeneous QKD: Different QKD systems with MDI-QKD and conventional point-to-point QKD protocols (e.g., BB84, COW, and GG02) may be used together to form a QKD network. It calls for the research on heterogeneous QKD networking, where the compatibility and interoperability should be investigated.

Moreover, the deployment of QKD networks for enabling highly secure communication links and various applications in 5G and beyond needs to be explored in the future.

IX. Conclusion

In this paper, we study the cost optimization when deploying QKD over an existing optical backbone network. Based on MDI-QKD, a new network architecture is described, where the hybrid trusted/untrusted relay scheme can be employed. Moreover, the node structures of the trusted relay and untrusted relay are detailed. The network, cost, and security models are formulated for deploying QKD with hybrid trusted/untrusted relays. An ILP model and a heuristic algorithm (i.e., CO-QBN) are presented to achieve the cost-optimized design. Simulation results verify the applicability of the presented ILP model and CO-QBN algorithm in different network topologies for a long run. The near-optimal characteristic of the CO-QBN algorithm is demonstrated. In particular, the deployment cost of a QKD backbone network can be saved up to 25% with the hybrid trusted/untrusted relay scheme relative to the purely trusted relay scheme, provided that the MDI-QKD scheme is technically more mature and its device cost can reach the level of conventional point-to-point QKD protocols in the future. In addition, a QKD backbone network based on the hybrid trusted/untrusted relay scheme can achieve a higher level of security than that based on the purely trusted relay scheme. Finally, some open issues in future work are also discussed.

References

[1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, no. 7285, pp. 45–53, Mar. 2010.

[2] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019.

[3] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[4] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, Apr. 2019.

[5] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photon.*, vol. 8, no. 8, pp. 595–604, Aug. 2014.

[6] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, Nov. 2016, Art. no. 16025.

[7] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: Challenges and solutions [Invited]," *Opt. Express*, vol. 26, no. 18, pp. 24260–24273, Sept. 2018.

[8] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[9] A. Boaron *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, Nov. 2018, Art. no. 190502.

[10] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Sept. 2017.

[11] 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, Jan. 1984, pp. 175–179.

[12] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett.*, vol. 87, no. 19, Nov. 2005, Art. no. 194108.

[13] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, Jan. 2002, Art. no. 057902.

[14] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," *Proc. SPIE, Quantum Inf. Comput. III*, vol. 5815, pp. 138–149, May 2005.

[15] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, July 2009, Art. no. 075001.

[16] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, May 2011.

[17] J. F. Dynes *et al.*, "Cambridge quantum network," *npj Quantum Inf.*, vol. 5, Nov. 2019, Art. no. 101.

[18] A. Aguado, V. López, D. López, M. Peev, A. Poppe, A. Pastor, J. Folgueira, and V. Martin, "The engineering of software-defined quantum key distribution networks," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 20–26, July 2019.

[19] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, no. 1, pp. 33–80, Mar. 2011.

[20] R. V. Meter and J. Touch, "Designing quantum repeater networks," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 64–71, Aug. 2013.

[21] Y. Hasegawa, R. Ikuta, N. Matsuda, K. Tamaki, H.-K. Lo, T. Yamamoto, K. Azuma, and N. Imoto, "Experimental time-reversed adaptive Bell measurement towards all-photonic quantum repeaters," *Nature Commun.*, vol. 10, Jan. 2019, Art. no. 378.

[22] Z.-D. Li, R. Zhang, X.-F. Yin, L.-Z. Liu, Y. Hu, Y.-Q. Fang, Y.-Y. Fei, X. Jiang, J. Zhang, L. Li, N.-L. Liu, F. Xu, Y.-A. Chen, and J.-W. Pan, "Experimental quantum repeater without quantum memory," *Nature Photon.*, vol. 13, no. 9, pp. 644–648, Sept. 2019.

[23] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, no. 7465, pp. 69–72, Sept. 2013.

[24] X. Tang, A. Wonfor, R. Kumar, R. V. Penty, and I. H. White, "Quantum-safe metro network with low-latency reconfigurable quantum key distribution," *J. Lightwave Technol.*, vol. 36, no. 22, pp. 5230–5236, Nov. 2018.

[25] A. Wonfor, C. White, A. Bahrami, J. Pearse, G. Duan, A. Straw, T. Edwards, T. Spiller, R. Penty, and A. Lord, "Field trial of multi-node, coherent-one-way quantum key distribution with encrypted 5x100G DWDM transmission system," in *Proc. Eur. Conf. Opt. Commun.*, Dublin, Ireland, Sept. 2019.

[26] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503.

[27] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, no. 1, Mar. 2016, Art. no. 011024.

[28] R. Valivarthi, P. Umesh, C. John, K. A. Owen, V. B. Verma, S. W. Nam, D. Oblak, Q. Zhou, and W. Tittel, "Measurement-device-independent quantum key distribution coexisting with classical communication," *Quantum Sci. Technol.*, vol. 4, no. 4, July 2019, Art. no. 045002.

[29] X.-T. Fang *et al.*, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nature Photon.*, vol. 14, no. 7, pp. 422–425, July 2020.

[30] J.-P. Chen *et al.*, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, no. 7, Feb. 2020, Art. no. 070501.

[31] Y. Ou, E. Hugues-Salas, F. Ntavou, R. Wang, Y. Bi, S. Yan, G. Kanellos, R. Nejabati, and D. Simeonidou, "Field-trial of machine learning-assisted quantum key distribution (QKD) networking with SDN," in *Proc. Eur. Conf. Opt. Commun.*, Rome, Italy, Sept. 2018.

[32] J. Niu, Y. Sun, Y. Zhang, and Y. Ji, "Noise-suppressing channel allocation in dynamic DWDM-QKD networks using LightGBM," *Opt. Express*, vol. 27, no. 22, pp. 31741–31756, Oct. 2019.

[33] Y. Cao, Y. Zhao, X. Yu, and Y. Wu, "Resource assignment strategy in optical networks integrated with quantum key distribution," *J. Opt. Commun. Netw.*, vol. 9, no. 11, pp. 995–1004, Nov. 2017.

[34] Y. Cao, Y. Zhao, Y. Wu, X. Yu, and J. Zhang, "Time-scheduled quantum key distribution (QKD) over WDM networks," *J. Lightwave Technol.*, vol. 36, no. 16, pp. 3382–3395, Aug. 2018.

[35] Y. Zhao, Y. Cao, W. Wang, H. Wang, X. Yu, J. Zhang, M. Tornatore, Y. Wu, and B. Mukherjee, "Resource allocation in optical networks secured by quantum key distribution," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 130–137, Aug. 2018.

[36] S. Bahrani, M. Razavi, and J. A. Salehi, "Wavelength assignment in hybrid quantum-classical networks," *Sci. Rep.*, vol. 8, Feb. 2018, Art. no. 3456.

[37] A. Aguado *et al.*, "Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources," *J. Lightwave Technol.*, vol. 35, no. 8, pp. 1357–1362, Apr. 2017.

[38] R. S. Tessinari *et al.*, "Field trial of dynamic DV-QKD networking in the SDN-controlled fully-meshed optical metro network of the Bristol city 5GUK test network," in *Proc. Eur. Conf. Opt. Commun.*, Dublin, Ireland, Sept. 2019.

[39] 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. Express*, vol. 25, no. 22, pp. 26453–26467, Oct. 2017.

[40] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Multi-tenant provisioning for quantum key distribution networks with heuristics and reinforcement learning: A comparative study," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 2, pp. 946–957, June 2020.

[41] Y. Cao, Y. Zhao, R. Lin, X. Yu, J. Zhang, and J. Chen, "Multi-tenant secret-key assignment over quantum key distribution networks," *Opt. Express*, vol. 27, no. 3, pp. 2544–2561, Feb. 2019.

[42] Y. Cao, Y. Zhao, X. Yu, and J. Zhang, "Multi-tenant provisioning over software defined networking enabled metropolitan area quantum key distribution networks," *J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. B31–B40, Mar. 2019.

[43] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "SDQaaS: software defined networking for quantum key distribution as a service," *Opt. Express*, vol. 27, no. 5, pp. 6892–6909, Mar. 2019.

[44] M. Mehic, P. Fazio, S. Rass, O. Maurhart, M. Peev, A. Poppe, J. Rozhon, M. Niemiec, and M. Voznak, "A novel approach to quality-of-service provisioning in trusted relay quantum key distribution networks," *IEEE/ACM Trans. Netw.*, vol. 28, no. 1, pp. 168–181, Feb. 2020.

[45] R. Wang *et al.*, "End-to-end quantum secured inter-domain 5G service orchestration over dynamically switched flex-grid optical networks enabled by a q-ROADM," *J. Lightwave Technol.*, vol. 38, no. 1, pp. 139–149, Jan. 2020.

[46] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "KaaS: Key as a service over quantum key distribution integrated optical networks," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 152–159, May 2019.

[47] K. Dong, Y. Zhao, T. Yang, Y. Li, A. Nag, X. Yu, and J. Zhang, "Tree-topology-based quantum-key-relay strategy for secure multicast services," *J. Opt. Commun. Netw.*, vol. 12, no. 5, pp. 120–132, May 2020.

[48] A. Aguado, V. Lopez, J. Martinez-Mateo, T. Szyrkowiec, A. Autenrieth, M. Peev, D. Lopez, and V. Martin, "Hybrid conventional and quantum security for software defined and virtualized networks," *J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 819–825, Oct. 2017.

[49] R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, "Topological optimization of quantum key distribution networks," *New. J. Phys.*, vol. 11, no. 7, July 2009, Art. no. 075002.

[50] 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, June 2019.

[51] F. Pederzolli, F. Faticanti, and D. Siracusa, "Optimal design of practical quantum key distribution backbones for securing core transport networks," *Quantum Rep.*, vol. 2, no. 1, pp. 114–125, Jan. 2020.

[52] X. Zou, X. Yu, Y. Zhao, A. Nag, and J. Zhang, "Collaborative routing in partially-trusted relay based quantum key distribution optical networks," in *Proc. Opt. Fiber Commun. Conf.*, San Diego, CA, USA, Mar. 2020, Art. no. M3K.4.

[53] "Overview on networks supporting quantum key distribution," Recommendation ITU-T Y.3800, Oct. 2019.

[54] C. E. Shannon, "Communication theory of secrecy systems," *The Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[55] W. Wang, F. Xu, and H.-K. Lo, "Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks," *Phys. Rev. X*, vol. 9, no. 4, Oct. 2019, Art. no. 041012.

[56] H. Liu *et al.*, "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels," *Phys. Rev. Lett.*, vol. 122, no. 16, Apr. 2019, Art. no. 160501.

[57] S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, and G. Franzl, "Perspectives and limitations of QKD integration in metropolitan area networks," *Opt. Express*, vol. 23, no. 8, pp. 10359–10373, Apr. 2015.

[58] T. A. Eriksson, R. S. Luis, B. J. Puttnam, G. Rademacher, M. Fujiwara, Y. Awaji, H. Furukawa, N. Wada, M. Takeoka, and M. Sasaki, "Wavelength division multiplexing of 194 continuous variable quantum key distribution channels," *J. Lightwave Technol.*, vol. 38, no. 8, pp. 2214–2218, Apr. 2020.

[59] "Functional requirements for quantum key distribution networks," Recommendation ITU-T Y.3801, Apr. 2020.

[60] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, "Integrating quantum key distribution with classical communications in backbone fiber network," *Opt. Express*, vol. 26, no. 5, pp. 6010–6020, Mar. 2018.

[61] C. le Quoc, P. Bellot, and A. Demaille, "Stochastic routing in large grid-shaped quantum networks," in *Proc. IEEE Int. Conf. Research, Innovation and Vision for the Future*, Hanoi, Vietnam, Mar. 2007, pp. 166–174.

[62] H. Wen, Z. Han, Y. Zhao, G. Guo, and P. Hong, "Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network," *Sci. China Ser. F-Inf. Sci.*, vol. 52, no. 1, pp. 18–22, Jan. 2009.

[63] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," *Nature Commun.*, vol. 8, Feb. 2017, Art. no. 13984.

[64] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, "Chip-based measurement-device-independent quantum key distribution," *Optica*, vol. 7, no. 3, pp. 238–242, Mar. 2020.

[65] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, "Experimental measurement-device-independent quantum digital signatures," *Nature Commun.*, vol. 8, Oct. 2017, Art. no. 1098.

Yuan Cao received the B.Eng. degree in optoelectronic information engineering from Nanjing University of Posts and Telecommunications, China, in 2016. He is currently pursuing the Ph.D. degree in information and communication engineering at Beijing University of Posts and Telecommunications, China. From June 2018 to August 2018, he was a Visiting Ph.D. Student at KTH Royal Institute of Technology, Sweden. From June 2019 to August 2019, he was a Visiting Ph.D. Student at the University of Southampton, U.K. His research interests include quantum key distribution networking, software defined networking, and optical network security.

Yongli Zhao (SM'15) is currently a Professor at Beijing University of Posts and Telecommunications. He received the Ph.D. degree from Beijing University of Posts and Telecommunications in 2010. From January 2016 to January 2017, he was a Visiting Associate Professor at the University of California, Davis. He has published more than 400 international journal and conference papers. His research focuses on software defined optical networks, elastic optical networks, datacenter networking, machine learning in optical networks, optical network security, and quantum key distribution networking.

Jun Li received the Ph.D. degree from the KTH Royal Institute of Technology, Sweden, in 2019. He was a Visiting Ph.D. Student with Princeton University, from September 2018 to March 2019. He is currently a Postdoctoral Researcher with the Chalmers University of Technology, Sweden. His research interests focus on fog/edge computing, optical network, and distributed machine learning.

Rui Lin (M'17) received the B.Eng. degree in electrical and information engineering from Huazhong University of Science and Technology, China, in 2011 and the Ph.D. degree in communication system from KTH Royal Institute of Technology, Sweden, in 2016. She is now working as a Postdoctoral Researcher in Department of Electrical Engineering, Chalmers University of Technology, Sweden. Her research interests include enabling technologies for high-speed optical communication networks and cyber security.

Jie Zhang is currently a Professor and Dean of the School of Electronic Engineering at Beijing University of Posts and Telecommunications. He received the Ph.D. degree in electromagnetic field and microwave technology from Beijing University of Posts and Telecommunications in 1998. He has published more than 400 technical papers, authored eight books, and submitted 17 ITU-T recommendation contributions and six IETF drafts. His research focuses on architecture, protocols, and standards for optical transport networks.

Jiajia Chen (SM'14) received the Ph.D. degree from KTH Royal Institute of Technology, Sweden, in 2009. Currently, she is a Professor in Chalmers University of Technology, Sweden. Her research interests broadly concern optical interconnect and transport networks for telecom and datacom, with a focus on various network aspects including agility, security, resource utilization, capacity, energy efficiency and cost efficiency.