Topological optimization of hybrid quantum key distribution networks

YAXING WANG, [1] QIONG LI, [1,*] HAOKUN MAO, [1] QI HAN, [1] FURONG HUANG, [2] AND HONGWEI XU [1]

[1] School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China
[2] School of International Studies, Harbin Institute of Technology, Harbin, China
[*] qiongli@hit.edu.cn

Abstract: With the growing complexity of quantum key distribution (QKD) network structures, aforehand topology design is of great significance to support a large-number of nodes over a large-spatial area. However, the exclusivity of quantum channels, the limitation of key generation capabilities, the variety of QKD protocols and the necessity of untrusted-relay selection, make the optimal topology design a very complicated task. In this research, a hybrid QKD network is studied for the first time from the perspective of topology, by analyzing the topological differences of various QKD protocols. In addition, to make full use of hybrid networking, an analytical model for optimal topology calculation is proposed, to reach the goal of best secure communication service by optimizing the deployment of various QKD devices and the selection of untrusted-relays under a given cost limit. Plentiful simulation results show that hybrid networking and untrusted-relay selection can bring great performance advantages, and then the universality and effectiveness of the proposed analytical model are verified.

1. Introduction

Quantum key distribution (QKD) technology, which generates information-theoretic secure (ITS) keys between a long distance communication pair based on the laws of quantum mechanics, has become one of the most promising technologies in quantum communication. However, it is necessary to establish QKD networks [1–9] based on multiple QKD devices to provide quantum key service for more users, since a QKD device can only provide quantum keys for a communication pair. In recent years, the number of nodes in experimental QKD networks has expanded from 6 [2, 10] to 56 [11], and the transmission distance has extended from 19.6 [12] to 2000 kilometers [11]. With the growing complexity of QKD network structures, the design from the perspective of topology is of great significance for quality assurance, cost control, and cycle reduction, etc [13, 14].

With the continuous development of QKD technology, more and more types of QKD protocols can be used to construct a QKD network. Different protocols vary greatly in terms of key generation capability, manufacturing cost, fiber dependency and so on. For example, a BB84-QKD device [15] has a relatively high key generation capability, but the required single-photon detectors are expensive. By contrast, a GG02-QKD device [16] does not require single photon detector, which reduces the manufacturing cost, but its key generation capability is lower, especially in the case of long optical fiber distance. Different from the previous two, a TF-QKD device [17] can achieve a relatively higher key generation rates in asymmetric fiber distances with a relatively low manufacturing cost, by overcoming the point-to-point rate-distance limit [18], but it does not work well in the symmetric case. Therefore, facing the diverse fiber distances in complex network topology and the limited cost for network construction, it is worth speculating that a hybrid QKD network composed of multi-type QKD protocols can provide better communication services.

To connect multiple QKD devices, the optical-switch, the quantum-relay, and the trusted-

relay are the three commonly used approaches [19–21]. Due to the scale limitation of optical-switches [22] and the technology immaturity of quantum-relays [23, 24], trusted-relay is the most practical approach at present [11]. This approach carries the risk of information leakage at trusted-relays. To reduce the risk, several efforts have been made in recent years [25–27], such as the exclusive-or based key storage [28] and the game-theory based multi-path transmission [29]. However, the premise of the exclusive-or strategy is that the network owner has an efficient node attack detection capability, while the precondition of the game-theory strategy is that the network adversary can only attack limited number of nodes. Therefore, the applicability of these strategies is still limited in the real-life multi-user QKD networks. In order to provide ITS communication service in a real-life hybrid QKD network, the credibility of each trusted-relay must be controlled, which leads to the introduction of credibility control cost. It is generally assumed that all relay nodes are trusted-relays in the previous researches related to trusted-relay based QKD networks [12, 14]. As a result, the total credibility control cost of a whole network is proportional to the total number of relay nodes. However, for a hybrid QKD network, untrusted-relays, which do not consume credibility control cost, can also be used to connect some types of QKD devices [30], such as MDI-QKD and TF-QKD. By selecting some cheap untrusted-relays to reduce the total number of trusted relays, the total credibility control cost can be effectively saved. Taking advantage of the saved cost to deploy more QKD devices can certainly generate more quantum keys. Therefore, in contrast to the traditional default scenario where all relay nodes are considered to be trusted-relays, it is worth speculating that efficient selection of untrusted-relays can provide better communication services.

The variety of QKD protocols and the necessity of untrusted-relay selection, coupled with several intrinsic characteristics of QKD devices, such as the exclusivity of quantum channels and the limitation of key generation capabilities [18,31–33], make the optimal design of a hybrid QKD network a very complicated task [34–38]. In this research, we study the optimal design of QKD network from the perspective of topology. The main function of topology design is to provide the best communication service within a given cost limit by carefully deploying QKD devices and selecting untrusted-relays. In the literature [3] and [39], several cost optimization models for QKD network construction have been designed through the deployment of QKD devices and the construction of new relay nodes. However, it is hard to construct a new relay node according to the optimal working distance calculated by literature [3] in a real network which is restricted by the physical geography. In addition, MDI-QKD protocol, TF-QKD protocol, and other QKD protocols that rely on two solid fibers have not been studied in these works. Furthermore, all nodes in their QKD networks are considered to be trusted-relays, i.e., the selection of untrusted-relays has not been considered.

- In this research, to study the hybrid QKD network, the topological differences between the client-to-client (C2C-QKD) protocol and the client-server-client (CSC-QKD) protocol were analyzed.
- To make full use of hybrid networking, an analytical model for optimal topology calculation was proposed to calculate the optimal network performance under a given cost limit, and then obtain the optimal deployment of various QKD devices and the selection of untrusted-relays.
- To verify the universality and effectiveness of this work, a comprehensive simulation based on random topology and real topology was designed. Simulation results demonstrated the advantages of hybrid networking and untrusted-relay selection.

The paper is organized as follows: In Section 2, the topological differences are presented in detail. Based on the method, an analytical model for optimal topology calculation are proposed in Section 3. In Section 4, the simulations of topology calculation, based on the proposed

analytical model, are presented and the results are analyzed. Section 5 presents the concluding remarks.

2. Topological differences of various QKD protocols

For all types of QKD protocols, quantum state transmission is an important step. Its dependence on quantum channels leads to a typical problem of quantum channel exclusiveness for QKD devices. To solve this problem, researchers have put forward many approaches, such as wavelength-division-multiplexing and orthogonal-frequency-division-multiplexing, to realize the multiplexing of quantum channels on existing optical fibers, so as to provide quantum keys without changing existing communication facilities. As a result, the dependence problem on the existing optical fibers, i.e. fiber dependency, emerges. According to the distinction on fiber dependency, existing various QKD protocols can be divided into C2C-QKD protocol and CSC-QKD protocol, as shown in Fig. 1.

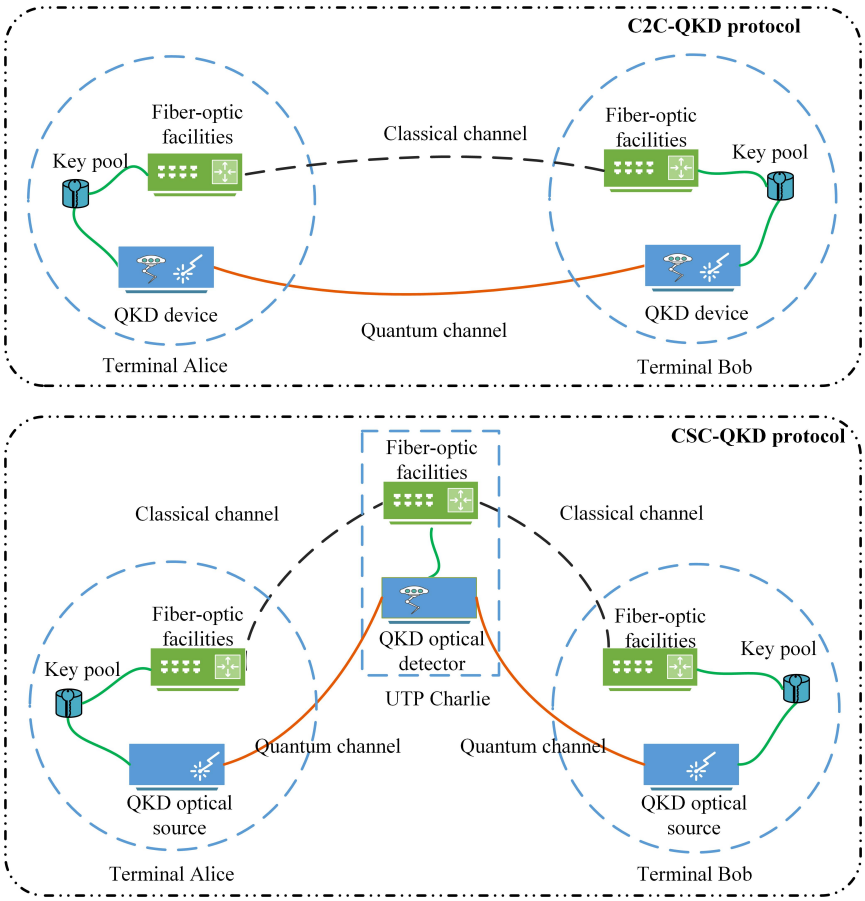

Fig. 1. The topological differences of various QKD protocols

The C2C-QKD protocol refers to the protocol that only one optical fiber is needed to connect a communication pair, such as BB84-QKD or E91-QKD. In contrast, the CSC-QKD protocol requires the participation of an untrusted third party (UTP), which is actually an untrusted-relay. Meanwhile, both of the two communication parties should connect to the UTP through one optical fiber. MDI-QKD and TF-QKD are the representatives of this kind. For demonstration purposes, we define the two communication parties of a C2C-QKD device as two C2C-clients

and label the quantum channel connecting two C2C-clients as a C2C-edge. Similarly, the two communication parties of a CSC-QKD device are defined as two CSC-clients, the UTP is called a CSC-server, and the two quantum channels connecting CSC-clients and CSC-server are labeled as two CSC-edges. In a hybrid QKD network, each node may plays one or more roles as a C2C-client, a CSC-client or a CSC-server, and each edge may contain one or more C2C-edges or CSC-edges.

3. An analytical model for optimal topology calculation

3.1. Notations and definitions

We summarize the notations used throughout the rest of this paper in Table 1 and make the following explanations.

Table 1. Main notations used in the research

Notation	Explanation	Value
$D^{s,t}$	Average communication demand of a communication pair (s,t)	R_0^+
$\beta^{s,t}$	Ratio of key length to plaintext length in the adopted encryption algorithm	R_0^+
$R_{(u,v)}$	Key generation capability of a C2C-QKD device arranged on the C2C-edge (u,v)	R_0^+
$\hat{R}_{(u,p,v)}$	Key generation capability of a CSC-QKD device arranged on the CSC-edge (u,p,v)	R_0^+
C	Available network construction cost	R_0^+
$S_{(u,v)}$	Number of C2C-QKD devices arranged on the C2C-edge (u,v)	N
$\hat{S}_{(u,p,v)}$	Number of CSC-QKD devices arranged on the CSC-edge (u,p,v)	N
$T(v)$	Credibility of node $v \in V$	$\{0,1\}$
$F_{(u,v)}^{s,t}$	Flow amount of a communication pair (s,t) passing through the C2C-edge (u,v)	R_0^+
$\hat{F}_{(u,p,v)}^{s,t}$	Flow amount of a communication pair (s,t) passing through the CSC-edge (u,p,v)	R_0^+
B	Global satisfaction degree of all communication demands	R_0^+

To expand the discussion more smoothly, it is necessary to explain in detail the definition and meaning of SoD, G-SoD and MG-SoD, the three main concepts used for topology evaluation, as shown below.

Definition 3.1.1 (SoD) *For a communication pair (s,t), its satisfaction degree of communication demand (SoD), $B^{s,t}$, is the ratio of its total key consumption, $A^{s,t}$, to its total key demand [11], i.e.,*

$$B^{s,t} = \frac{A^{s,t}}{D^{s,t} \cdot \beta^{s,t}}, \tag{1}$$

where $A^{s,t}$ can be calculated by the total difference between the flows into and out of the source node s, i.e.,

$$A^{s,t} = \sum_{v \in V} \left[F^{s,t}_{(s,v)} - F^{s,t}_{(v,s)} \right] + \sum_{p \in V, v \in V} \left[\hat{F}^{s,t}_{(s,p,v)} - \hat{F}^{s,t}_{(v,p,s)} \right]. \tag{2}$$

Definition 3.1.2 (G-SoD) *For a QKD network with a given topology $G = (V, E)$, its global satisfaction degree of all communication demands (G-SoD), B, is defined as the worst performance of all communication pairs [11]. Thus, B can be calculated by the minimum value of all SoDs, i.e.,*

$$B = \min_{s \in V, t \in V} B^{s,t} = \min_{s \in V, t \in V} \frac{A^{s,t}}{D^{s,t} \cdot \beta^{s,t}}. \tag{3}$$

Definition 3.1.3 (MG-SoD) *For a QKD network topology $G = (V, E)$, its optimal performance is defined as the maximum of all possible G-SoDs (MG-SoD), each of which is defined as the worst performance of all communication pairs over a possible flow assignment [11].*

3.2. The proposed analytical model

To make full use of hybrid networking, an analytical model, which is essentially an optimization formulation, is designed to solve the problem of the optimal deployment of various QKD devices and the selection of untrusted-relays for a hybrid QKD network.

The input items of this formulation mainly include the existing classical network, the communication demand, the key generation capability and the limited construction cost. (i) The existing classical network is represented as a directed graph $G = (V, E)$. Then, the set of all optional C2C-edges is E and the set of all optional CSC-edges is $\hat{E} = \{(u, p, v) \,|\, (u, p) \in E, (p, v) \in E\}$. (ii) The communication demand is defined as $D^{s,t}$ and the key consumption ratio as $\beta^{s,t}$. Therefore, the requested key demand is $D^{s,t} \cdot \beta^{s,t}$ for each communication pair (s, t) $(s \in V, t \in V)$. In particular, $\beta^{s,t} = 1$ indicates that the one-time-pad algorithm is adopted to achieve ITS communication and $\beta^{s,t} = 0$ indicates that the adopted encryption algorithm does not require quantum keys. (iii) The key generation capability for each C2C-QKD device arranged on the C2C-edge $(u, v) \in E$ is denoted as $R_{(u,v)}$, and the key generation capability for each CSC-QKD device arranged on the CSC-edge $(u, p, v) \in \hat{E}$ is denoted as $\hat{R}_{(u,p,v)}$. (iv) The total cost for QKD network construction is limited to C, which mainly includes the manufacturing cost of QKD devices and the credibility control cost of trusted-relays.

The decision variables of this formulation mainly contain three types: integer variable, boolean variable and continuous variable. (i) The integer variable $S_{(u,v)}$ represents the number of C2C-QKD devices arranged on the C2C-edge (u, v), and $\hat{S}_{(u,p,v)}$ represents the number of CSC-QKD devices arranged on the CSC-edge (u, p, v). (ii) The boolean variable $T(v)$ indicates whether node v is a trusted-relay and whether credibility control is required for this node. (iii) The continuous variable $F^{s,t}_{(u,v)}$ represents the flow amount of the communication pair (s, t) [11, 40, 41] passing through the C2C-edge (u, v), $\hat{F}^{s,t}_{(u,p,v)}$ represents the flow amount of the communication pair (s, t) passing through the CSC-edge (u, p, v), and B represents the quality of a QKD network topology, which can be measured by the G-SoD [11].

The complete formulation is then given by,

Maximize:

$$B. \tag{4}$$

Subject to:

$$\forall (u, v) \in E, 0 \leq \sum_{s \in V, t \in V} \left[F^{s,t}_{(u,v)} + F^{s,t}_{(v,u)} \right] \leq S_{(u,v)} R_{(u,v)} + S_{(v,u)} R_{(v,u)}, \tag{5}$$

$$\forall (u, p, v) \in \hat{E}, 0 \leq \sum_{s \in V, t \in V} \left[\hat{F}^{s,t}_{(u,p,v)} + \hat{F}^{s,t}_{(v,p,u)} \right] \leq \hat{S}_{(u,p,v)} \hat{R}_{(u,p,v)} + \hat{S}_{(v,p,u)} \hat{R}_{(v,p,u)}, \tag{6}$$

$$\forall s \in V, \forall t \in V, \forall u \in (V - \{s,t\}), \sum_{v \in V} \left[F^{s,t}_{(u,v)} - F^{s,t}_{(v,u)} \right] + \sum_{p \in V, v \in V} \left[\overline{F}^{s,t}_{(u,p,v)} - \overline{F}^{s,t}_{(v,p,u)} \right] = 0, \tag{7}$$

$$\forall s \in V, \forall t \in V, \sum_{v \in V} \left[F^{s,t}_{(s,v)} - F^{s,t}_{(v,s)} \right] + \sum_{p \in V, v \in V} \left[\hat{F}^{s,t}_{(s,p,v)} - \hat{F}^{s,t}_{(v,p,s)} \right] = A^{s,t}, \tag{8}$$

$$\forall s \in V, \forall t \in V, \sum_{v \in V} \left[F^{s,t}_{(t,v)} - F^{s,t}_{(v,t)} \right] + \sum_{p \in V, v \in V} \left[\hat{F}^{s,t}_{(t,p,v)} - \hat{F}^{s,t}_{(v,p,t)} \right] = -A^{s,t}, \tag{9}$$

$$\forall s \in V, \forall t \in V, A^{s,t} - B \cdot D^{s,t} \cdot \beta^{s,t} \geq 0, \tag{10}$$

$$\sum_{(u,v) \in E} S_{(u,v)} + q_1 \sum_{(u,p,v) \in \hat{E}} \hat{S}_{(u,p,v)} + q_2 \sum_{v \in V} T(v) - C \leq 0, \tag{11}$$

$$\forall v \in V, T(v) = \begin{cases} 0 & \text{if } I(v) = 0, \\ 1 & \text{if } I(v) \neq 0, \end{cases} \tag{12}$$

where

$$I(v) = \sum_{(u,v) \in E} S_{(u,v)} + \sum_{(v,u) \in E} S_{(v,u)} + \sum_{(u,p,v) \in \hat{E}} \hat{S}_{(u,p,v)} + \sum_{(v,p,u) \in \hat{E}} \hat{S}_{(v,p,u)}. \tag{13}$$

The objective function is expressed in Eq. (4), which maximizes the G-SoD. Constraints Eqs. (5, 6) state the capacity constraint condition, i.e., the total flow amount through an edge must be lower than the total key generation capability on this edge. Constraint Eq. (7) expresses the flow conservation condition, i.e., the total flow amount that enters a non-source-sink node must be equal to the total flow amount that exits this node. Constraints Eqs. (8-10) prove that sufficient key materials from the source node to the sink one is available to satisfy the key demand between the two nodes. Constraint Eq. (11) requires the actual cost must be no higher than the limited cost. Here, we use the price of a C2C-QKD device as the basis of cost calculation. Besides, the price of a CSC-QKD device is assumed to be q_1 times the base value, and the credibility control cost of a trusted-relay be q_2 times the base value. Constraint Eq. (12) carries out the selection of untrusted-relays, which have neither been C2C-client nor CSC-Client.

In this formulation, all other constraints are linear functions, except the Eq. (12) which is a piecewise function. To facilitate the solution, we transform the Eq. (12) into a linear expression by means of approximation, making this formulation a standard mixed-integer linear programming (MILP) model. More specifically, the Eq. (12) is rewritten as Eq. (14) by introducing additional boolean decision variable $T'(v)$ and continuous decision variable $T''(v)$, where M is an arbitrarily large real number.

$$\begin{cases} \forall v \in V, T'(v) + T''(v) = 1, \\ \forall v \in V, I(v) - M \cdot T(v) \leq 0, \\ \forall v \in V, I(v) + T'(v) - T''(v) \geq 0. \end{cases} \tag{14}$$

The decision variables of this standard MILP formulation are listed below:

$$\begin{cases} B \in R_0^+, \\ \forall (u,v) \in E, \forall s \in V, \forall t \in V, F_{(u,v)}^{s,t} \in R_0^+, \\ \forall (u,p,v) \in \hat{E}, \forall s \in V, \forall t \in V, \hat{F}_{(u,p,v)}^{s,t} \in R_0^+, \\ \forall (u,v) \in E, S(u,v) \in N, \\ \forall (u,p,v) \in \hat{E}, \hat{S}(u,p,v) \in N, \\ \forall v \in V, T(v) \in \{0,1\}, \\ \forall v \in V, T'(v) \in \{0,1\}, \\ \forall v \in V, T''(v) \in R_0^+. \end{cases} \tag{15}$$

As a typical MILP model, this formulation can be solved by a mature linear programming solver, Gurobi [42, 43]. After optimization, the proposed model is convenient to retrieve the MG-SoD (i.e., the objective function value), the number of QKD devices to be installed on each edge (i.e., $S_{(u,v)}$ and $\hat{S}_{(u,p,v)}$), the nodes to be selected as untrusted-relays (i.e., $T(v)$), and the paths to be selected for each communication pair to route the encrypted messages (i.e., $F_{(u,v)}^{s,t}$ and $\hat{F}_{(u,p,v)}^{s,t}$).

4. Simulation results and analysis

4.1. Optimal topology calculation of several random graphs

We evaluate the calculation results of our proposed analytical model on 13 random graphs, which are generated based on the ER model [44, 45]. These random graphs are set as follows: each family consists of 10 instances with a fixed number of nodes, an average nodal degree of 3, a set of edge lengths uniformly distributed at $[10, 500]$ kilometers, and a uniform traffic matrix established at $[100, 500]$ kbps between one fifth of nodes allowing the remaining four-fifths the opportunity to act as untrusted-relays. The simulation platform adopted in this research is detailed in Table 2.

Table 2. The simulation platform

	Parameter	Value
CPU	Version	Intel(R) Core(TM) i9-9820X
	Performance	10-Cores@3.3GHz
Gurobi	TimeLimit	7200s
	SolutionLimit	200
	MIPGap	0.01

In addition, we adopt the decoy-QKD protocol [38] to prepare C2C-QKD devices, and the SNS-TF-QKD [17] protocol to prepare CSC-QKD devices. To simplify the analysis, we assume that the parameters of all C2C-QKD devices are the same, and the parameters of all CSC-QKD devices are also the same. It should be noted that the proposed analytical model supports the configuration of different parameter setting for each QKD device. The main cost of a decoy-QKD device mainly comes from two single-photon detectors, similarly, the main cost of a SNS-TF-QKD device also mainly comes from the same detectors. Therefore, q_1 is assumed to

be 1, by taking the price of a decoy-QKD device as the basis of cost calculation. Considering the complexity of credibility control, which is usually realized by physical protection [46–50], q_2 is assumed to be 100. In addition, the overall cost for network construction is limited to 10000.

To demonstrate the advantages of hybrid networking and untrusted-relay selection clearly, the average values of all MG-SoDs obtained from 13 families of random graphs are standardized. Specifically, the simulation result in the case of hybrid networking and untrusted-relay selection is normalized as 100%, and the remaining results are normalized as the ratio to the above values, for each graph size.

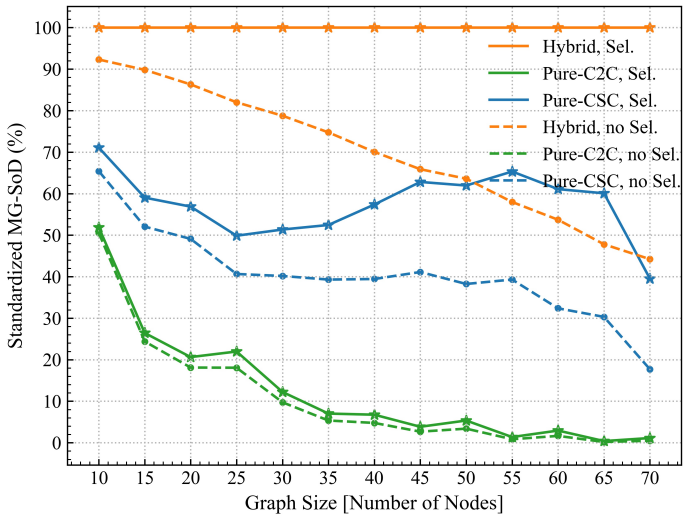

Fig. 2. Standardized MG-SoDs. The orange curves show the values for hybrid networks which contains both CSC-QKD and C2C-QKD devices; the blue curves denote the values for pure-CSC networks consisting of CSC-QKD devices only; the green curves denote the values for pure-C2C networks consisting of C2C-QKD devices only. The solid lines and dotted lines represent the cases with or without untrusted-relay selection respectively.

In Fig. 2, we report the standardized MG-SoDs of hybrid networks, pure-C2C networks and pure-CSC networks versus the graph size with or without untrusted-relay selection, respectively. As can be seen from the figure, higher MG-SoDs can be achieved when using multi-type QKD protocols: the value of hybrid network curves, which are orange, is always higher than that of green and blue curves. Higher MG-SoDs can be achieved by carefully selecting untrusted-relays: the value of the solid lines is always higher than the dotted lines. In addition, as the number of nodes increases, the performance of pure-C2C networks drops sharply, while such performance drop of pure-CSC networks is not always obvious. Furthermore, without untrusted-relay selection, the performances of all three types of QKD networks decrease monotonically with the increase of graph size.

To show the solving difficulty of our proposed analytical model more intuitively, we report the runtime results of different networking schemes in Fig. 3. As can be seen from the figure, the addition of hybrid networking and untrusted-relay selection makes the solving more difficult: the value of hybrid network curves, which are orange, is always higher than that of green and blue curves, and the value of the solid lines is always higher than the dotted lines. More obviously, as the number of nodes increases, the runtime of hybrid networks with untrusted-relay selection is always the longest, followed by the pure-CSC networks with untrusted-relay selection. By contrast, the runtimes of the remaining four schemes are much shorter, because they have fewer decision variables and fewer constraints. In addition, the optimal solution cannot be obtained

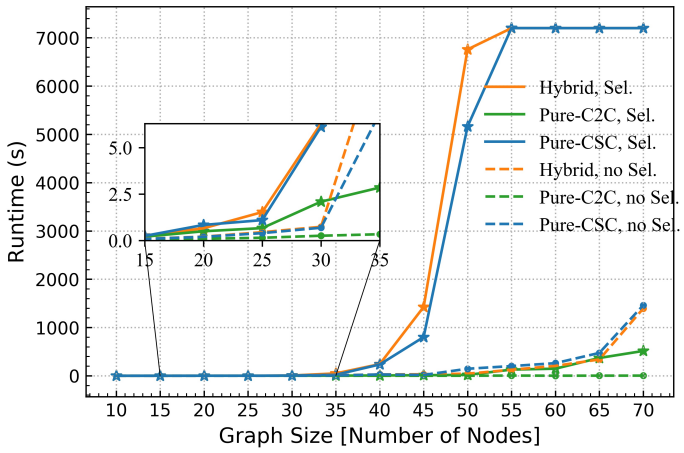

Fig. 3. Runtimes of different networking schemes. The orange curves show the values for hybrid networks; the blue curves denote the values for pure-CSC networks; the green curves denote the values for pure-C2C networks. The solid lines and dotted lines represent the cases with or without untrusted-relay selection respectively.

within 7200 seconds, when the number of nodes reaches 55. It is worth to mention that, it is essential to design corresponding heuristic algorithm [51, 52] to accelerate the calculation of optimal solution for large-scale network construction, which is also the research focus of our future work.

4.2. Optimal topology calculation of a real NSFNET topology

Although the above results are sufficient to prove the universality of this study, another simulation based on a real NSFNET topology (14 nodes and 21 edges) [11], as shown in Fig. 4, is conducted to further verify the effectiveness of the proposed analytical model.

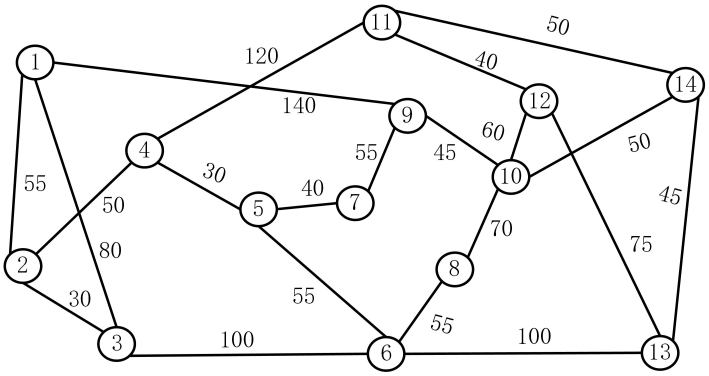

Fig. 4. Topology of NSFNET network.

Under the same assumptions, the corresponding optimal design is shown in Table 3, where Hyd. SoD, C2C. SoD, and CSC. SoD are used to indicate the MG-SoDs of hybrid network, pure-C2C network and pure-CSC network, respectively. From the data in the table, it can be concluded that both the hybrid networking and the untrusted-relay selection play a critical role in optimal topology design; therefore, the effectiveness of this study is verified.

Furthermore, it should be pointed out that, although the above simulation only gives the results of a set of specific input parameters due to the length limit, the conclusions are also established

Table 3. Optimal design under NSFNET topology

Selection	Hyd. SoD	C2C. SoD	CSC. SoD
No	828.12	740.95	335.93
Yes	915.65	785.09	383.37

for various input parameters.

5. Conclusion

In conclusion, we have proposed an analytical model to find the optimal deployment of various QKD devices and the selection of untrusted-relays under a given cost limit, and then to create a high-quality hybrid QKD network with the existing classical network. Through simulation, the universality and effectiveness of this study have been verified. In the process of research, the proposed model is calculated by using existing computing tools, Gurobi. However, in the face of large-scale QKD networks, specific heuristic algorithms should be designed to accelerate the calculation of the proposed model, which is also the research focus of our future work. In addition, to further improve the topology performance, we will study the physical protection of trusted-relays thoroughly based on existing works, to quantify and reduce the physical protection cost in our future work. We anticipate that the proposed model could contribute a significance for researchers to accelerate the construction process of QKD networks.

Funding

Space Science and Technology Advance Research Joint Funds (6141B06110105); National Natural Science Foundation of China (NSFC) (61301099).

Disclosures

The authors declare no conflicts of interest.

References

1. C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the darpa quantum network," in *Quantum Information and computation III,* vol. 5815 (International Society for Optics and Photonics, 2005), pp. 138–149.
2. A. Poppe, M. Peev, and O. Maurhart, "Outline of the secoqc quantum-key-distribution network in vienna," Int. J. Quantum Inf. **6**, 209–218 (2008).
3. R. Alleaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, "Topological optimization of quantum key distribution networks," New J. Phys. **11**, 075002 (2009).
4. M. Fujiwara, H. Ishizuka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, and A. Tajima, "Field demonstration of quantum key distribution in the tokyo qkd network," in *International Quantum Electronics Conference,* (Optical Society of America, 2011), p. I403.
5. H. Yin, T. Chen, Z. Yu, H. Liu, L. You, Y. Zhou, S. Chen, Y. Mao, M. Huang, and W. Zhang, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Phys. review letters **117**, 190501 (2016).
6. S. Liao, W. Cai, W. Liu, L. Zhang, Y. Li, J. Ren, J. Yin, Q. Shen, Y. Cao, and Z. Li, "Satellite-to-ground quantum key distribution," Nature **549**, 43 (2017).
7. S. Liao, W. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J. Ren, and W. Liu, "Satellite-relayed intercontinental quantum network," Phys. review letters **120**, 030501 (2018).
8. Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, and A. Murakami, "10-mb/s quantum key distribution," J. Light. Technol. **36**, 3427–3433 (2018).
9. Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, and Z. Wang, "Continuous-variable qkd over 50 km commercial fiber," Quantum Sci. Technol. **4**, 035006 (2019).
10. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, and A. Tanaka, "Field test of quantum key distribution in the tokyo qkd network," Opt. express **19**, 10387–10409 (2011).
11. Q. Li, Y. Wang, H. Mao, J. Yao, and Q. Han, "Mathematical model and topology evaluation of quantum key distribution network," Opt. Express **28**, 9419–9434 (2020).

12. M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, and J. Dynes, "The secoqc quantum key distribution network in vienna," New J. Phys. **11**, 075001 (2009).
13. M. Dianati, R. Alléaume, M. Gagnaire, and X. Shen, "Architecture and protocols of the future european quantum key distribution network," Secur. Commun. Networks **1**, 57–74 (2008).
14. E. Diamanti, H. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Inf. **2**, 16025 (2016).
15. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing." Theor. Comput. Sci. **560**, 7–11 (2014).
16. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. review letters **88**, 057902 (2002).
17. F. Grasselli, A. Navarrete, and M. Curty, "Asymmetric twin-field quantum key distribution," New J. Phys. **21**, 113032 (2019).
18. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).
19. P. D. Townsend, "Quantum cryptography on multiuser optical fibre networks," Nature **385**, 47 (1997).
20. P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, "Comparison of four multi-user quantum key distribution schemes over passive optical networks," J. lightwave technology **23**, 268 (2005).
21. L. Ma, H. Xu, and X. Tang, "Polarization recovery and auto-compensation in quantum key distribution network," in *Quantum Communications and Quantum Imaging IV,* vol. 6305 (International Society for Optics and Photonics, 2006), p. 630513.
22. P. Toliver, R. J. Runser, T. E. Chapuran, J. L. Jackel, T. C. Banwell, M. S. Goodman, R. J. Hughes, C. G. Peterson, D. Derkacs, and J. E. Nordholt, "Experimental investigation of quantum key distribution through transparent optical switch elements," IEEE Photonics Technol. Lett. **15**, 1669–1671 (2003).
23. L. Chen, H. Yong, P. Xu, X. Yao, T. Xiang, Z. Li, C. Liu, H. Lu, N. Liu, and L. Li, "Experimental nested purification for a linear optical quantum repeater," Nat. Photonics **11**, 695 (2017).
24. X.-M. Hu, C. Zhang, C.-J. Zhang, B.-H. Liu, Y.-F. Huang, Y.-J. Han, C.-F. Li, and G.-C. Guo, "Experimental certification for nonclassical teleportation," Quantum Eng. **1**, e13 (2019).
25. M. Fitzi, M. Franklin, J. Garay, and S. H. Vardhan, "Towards optimal and efficient perfectly secure message transmission," in *Theory of Cryptography Conference,* (Springer, 2007), pp. 311–322.
26. Y. Wang and Y. Desmedt, "Perfectly secure message transmission revisited," IEEE Transactions on Inf. Theory **54**, 2582–2595 (2008).
27. P. Schartner, S. Rass, and M. Schaffer, "Quantum key management," in *Applied Cryptography and Network Security,* (InTech, 2012), p. 227.
28. P. Schartner and S. Rass, "How to overcome the'trusted node model'in quantum cryptography," in *2009 International Conference on Computational Science and Engineering,* vol. 3 (IEEE, 2009), pp. 259–262.
29. S. Rass and P. Schartner, "A unified framework for the analysis of availability, reliability and security, with applications to quantum networks," IEEE Transactions on Syst. Man, Cybern. Part C (Applications Rev. **41**, 107–119 (2010).
30. H.-K. Lo, W. Wang, and F. Xu, "Scalable measurement-device-independent quantum key distribution networks with untrusted relays," in *Optical Fiber Communication Conference,* (Optical Society of America, 2020), pp. M1E–2.
31. 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 Transactions on Netw. **28**, 168–181 (2019).
32. Q. Li, X. Wen, H. Mao, and X. Wen, "An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution," Quantum Inf. Process. **18**, 25 (2019).
33. H. Mao, Q. Li, Q. Han, and H. Guo, "High-throughput and low-cost ldpc reconciliation for quantum key distribution," Quantum Inf. Process. **18**, 232 (2019).
34. O. Maurhart, C. Pacher, A. Happe, T. Lor, C. Tamas, A. Poppe, and M. Peev, "New release of an open source qkd software: design and implementation of new algorithms, modularization and integration with ipsec," in *Proc. Qcrypt,* (Citeseer, 2013), p. 1.
35. Q. Han, L. Yu, W. Zheng, N. Cheng, and X. Niu, "A novel qkd network routing algorithm based on optical-path-switching," J. Inf. Hiding Multimed. Signal Process. **5**, 13–19 (2014).
36. C. Yang, H. Zhang, and J. Su, "The qkd network: model and routing scheme," J. Mod. Opt. **64**, 2350–2362 (2017).
37. M. Mehic, O. Maurhart, S. Rass, and M. Voznak, "Implementation of quantum key distribution network simulation module in the network simulator ns-3," Quantum Inf. Process. **16**, 253 (2017).
38. Y. Wang, Q. Li, Q. Han, and Y. Wang, "Modeling and simulation of practical quantum secure communication network," Quantum Inf. Process. **18**, 278 (2019).
39. F. Pederzolli, F. Faticanti, and D. Siracusa, "Optimal design of practical quantum key distribution backbones for securing coretransport networks," Quantum Reports **2**, 114–125 (2020).
40. A. Schrijver, "On the history of the transportation and maximum flow problems," Math. Program. **91**, 437–445 (2002).
41. S. Han, Z. Peng, and S. Wang, "The maximum flow problem of uncertain network," Inf. Sci. **265**, 167–175 (2014).
42. Z. Li, Q. Chen, and V. Koltun, "Combinatorial optimization with graph convolutional networks and guided tree

search," in *Advances in Neural Information Processing Systems,* (2018), pp. 539–548.
43. W. E. Helm and J.-E. Justkowiak, "Extension of mittelmanns benchmarks: Comparing the solvers of sas and gurobi," in *Operations Research Proceedings 2016,* (Springer, 2018), pp. 607–613.
44. D. Garlaschelli, "The weighted random graph model," New J. Phys. **11**, 073005 (2009).
45. M. Drobyshevskiy and D. Turdakov, "Random graph modeling: A survey of the concepts," ACM Comput. Surv. (CSUR) **52**, 1–36 (2019).
46. Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: challenges and solutions," Opt. express **26**, 24260–24273 (2018).
47. P. Techateerawat, "Network management system for quantum key distribution," in *The 8th Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI) Association of Thailand-Conference 2011,* (IEEE, 2011), pp. 292–295.
48. P. Evans, G. Peterson, T. Morgan, K. Jones, S. Morrison, R. ell, and N. Peters, "Demonstration of a quantum key distribution trusted node on an electric utility fiber network," in *2019 IEEE Photonics Conference (IPC),* (IEEE, 2019), pp. 1–2.
49. H. Zhang, J. Wang, K. Cui, C. Luo, S. Lin, L. Zhou, H. Liang, T. Chen, K. Chen, and J. Pan, "A real-time qkd system based on fpga," J. Light. Technol. **30**, 3226–3234 (2012).
50. L. O. Mailloux, J. D. Morris, M. R. Grimaila, D. D. Hodson, D. R. Jacques, J. M. Colombi, C. V. Mclaughlin, and J. A. Holes, "A modeling framework for studying quantum key distribution system implementation nonidealities," IEEE Access **3**, 110–130 (2015).
51. K. Holmberg and D. Yuan, "A lagrangian heuristic based branch-and-bound approach for the capacitated network design problem," Oper. Res. **48**, 461–481 (2000).
52. M. Yaghini, M. Momeni, and M. Sarmadi, "A simplex-based simulated annealing algorithm for node-arc capacitated multicommodity network design," Appl. Soft Comput. **12**, 2997–3003 (2012).