Research Article | Vol. 28, No. 7 / 30 March 2020 / Optics Express 9419

Optics EXPRESS

Mathematical model and topology evaluation of quantum key distribution network

QIONG LI, YAXING WANG,* HAOKUN MAO, JIAMENG YAO, AND QI HAN

Information Countermeasure Technique Institute, School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150080, China

*yaxwang@163.com

Abstract: Due to the intrinsic point-to-point characteristic of quantum key distribution (QKD) systems, it is necessary to study and develop QKD network technology to provide a secure communication service for a large-scale of nodes over a large area. Considering the quality assurance required for such a network and the cost limitations, building an effective mathematical model of a QKD network becomes a critical task. In this paper, a flow-based mathematical model is proposed to describe a QKD network using mathematical concepts and language. In addition, an investigation on QKD network topology evaluation was conducted using a unique and novel QKD network performance indicator, the *Information-Theoretic Secure communication bound*, and the corresponding linear programming-based calculation algorithm. A large number of simulation results based on the SECOQC network and NSFNET network validate the effectiveness of the proposed model and indicator.

1. Introduction

With the rapid development and increasing applicability of quantum key distribution (QKD) technology [1–4], its intrinsic point-to-point feature [5] has become one of the major bottlenecks limiting the scale of its application. To overcome the limitation on the quantity of nodes [6] and communication distance, the construction of a QKD network with multiple QKD systems was an inevitable development trend. The QKD network in this paper is defined as a network that provides a secure communication service, utilizing the keys generated by QKD systems [7]. In order to explore the physical feasibility of QKD networking, many practical QKD networks [8–13] have been constructed in recent years. In the last decade, the number of nodes in existing QKD networks has expanded from 6 [10,14] to 56 nodes [15] and the communication distance has extended from 19.6 [16] to 2000 km [15]. With the growing coverage and complexity of QKD networks, effective modeling is crucial for functional verification, quality assurance, cost control, cycle shortening, etc. [17,18].

The two primary approaches of network modeling include simulation models and mathematical models. Unlike traditional communication networks, the relevant research of QKD networks has not drawn much attention [7,19–23]. In 2017, Mehic et. al. designed a QKD network simulation model, QKDNetSim [23], based on the classical Network Simulator-version 3 [24], to evaluate and validate a network solution at a low cost. Although QKDNetSim could simulate the key generation and secure communication processes, it could not accurately reflect the practical performance of a QKD network, owing to its neglect of the actual key generation capability and volatile communication demand of the QKD network. In order to reflect the state of a practical network, we designed a practical QKD network simulation model in our previous work [7]. In this model, the point-to-point key generation capability was modeled by the Gottesman-Lo-Lutkenhaus-Preskill (GLLP) theory [25] and the volatile end-to-end communication demand was modeled by the Poisson stochastic process. Although our previous work enhanced the accuracy

#387697 https://doi.org/10.1364/OE.387697
Journal © 2020 Received 10 Jan 2020; revised 7 Mar 2020; accepted 10 Mar 2020; published 18 Mar 2020

of the QKDNetSim, the inherent shortcomings of a simulation approach still exist, such as the empirical results, the difficult global optimal solution, etc.

A mathematical model, however, is a general mathematical abstraction of a QKD network, and therefore makes it possible to theoretically evaluate the performance of a QKD network and obtain the global optimal solution, etc. This topic has not been studied thoroughly so far, though there have been many articles in the area of QKD networking in the past two years, especially about the architecture [26], software-defined network [27,28], routing [29], key management [30,31] and key resource allocation [32]. According to the results of our simulation model [7], the performance of a practical QKD network primarily depends on how its key generation capability satisfies the communication demand. With emphasis on this characteristic, we are motivated to study the mathematical model of a QKD network, and its applications.

- In this paper, a flow-based mathematical (FM) model is proposed. In the model, a QKD network was abstracted as the graph $G = (V, E, F)$, with the node set V, the edge set E and the *QKD-flow* set F. According to the analysis of QKD network characteristics, the detailed attributes of the node and edge were analyzed. Furthermore, the *QKD-flow* was defined in reference to the generic *traffic-flow* [33,34], which is a unique component of a QKD network, compared to a classical network.
- Based on the FM model, an investigation on QKD network topology evaluation was conducted by proposing the indicator, the *Information-Theoretic Secure (ITS) communication bound*, and the corresponding calculation algorithm. The indicator is designed to theoretically quantify the optimal performance of a QKD network topology [35]. The calculation is inspired by the linear programming algorithm.
- In order to verify the validity and necessity of the proposed FM model and performance indicator, two typical topology evaluation tasks, based on the SECOQC network [16] and NSFNET network [36], were designed and simulated. The simulation results demonstrated the advantages of the FM model and *ITS communication bound*.

The paper is organized as follows: In Section 2, some related literature is discussed. In Section 3, the FM model is presented in detail. Based on the model, a unique QKD network performance indicator and the corresponding linear programming-based calculation algorithm are proposed in Section 4. In Section 5, the simulations of topology evaluation, based on the FM model, are presented and the results are analyzed. Section 6 presents the concluding remarks.

2. Related literature

In this section, related literature is reviewed and analyzed. The construction modes, application modes, and architecture models of a QKD network are discussed and the generic maximum-flow problem, which is usually used for task allocation, is introduced as one of the theoretical bases of the FM model.

2.1. Construction modes of QKD network

Construction modes used in existing QKD networks are divided into three main categories: optical switching, quantum relay, and trusted relay [37–39]. Because an optical switching device cannot break the scale limitation [40] and the core technique of quantum relay is still far from mature [41,42], the trusted relay is the most common construction mode at present.

2.2. Application modes of QKD network

Application modes used in existing QKD networks primarily include the key-by-key (also called key relay) [22] and data-by-data (also called hop-by-hop) [23] modes. The main difference

Optics EXPRESS

between these modes is how the communication is established. The key-by-key mode, used in the Tokyo network [14], can better retain the classical network protocol. However, in this mode, the number of key pools configured for each communication node is proportional to the number of potential communication parties. This requires a large memory capacity, which is impractical in a large-scale QKD network. In the data-by-data mode, which was used in the SECOQC network [43], the number of key pools for each node is only related to the degree of the node [44]. This mode can greatly reduce the memory demand and, thus, increase the availability of a large-scale QKD network. Therefore, the data-by-data mode is more appropriate at present.

2.3. Architecture models of QKD network

Compared to a traditional communication network, the secure communication process between the end-to-end communication parties of a QKD network needs to consume the quantum keys generated by the point-to-point links. Therefore, a two-layer architecture model of a QKD network was proposed in our previous work [7], which is shown in Fig. 1. In this model, end-to-end secure communication and point-to-point key generation proceed in the classical layer and the quantum layer, respectively.

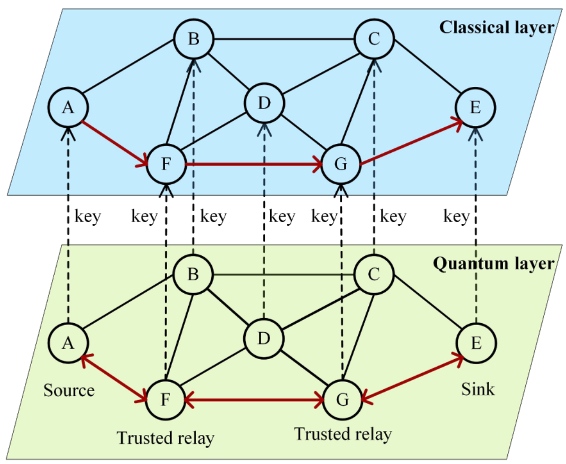


Fig. 1. Two-layer architecture model of a QKD network [7]

Because the point-to-point key generation capability of a QKD system is extremely limited by the length of the quantum channel [45,46] and is markedly lower than the capacity of the classical channel [47], the performance of a QKD network is determined by the alignment of the communication demand and the key generation capability. Referring to our previous work [7], the point-to-point key generation capability of the quantum layer can be obtained by the common calculation method used for the secure key rate of a QKD system, such as GLLP theory [25,48] and the universal composable framework [49]. Assuming that the double decoy state protocol is adopted in the QKD network and the Chernoff bound [50] is used to estimate the finite code length effect [51,52], the key generation capability R_{key} can be calculated as,

$$R_{key} = \max\left\{f_{req}R_L, 0\right\}, \tag{1}$$

where R_L represents the lower bound of the key generation capability for a photon, calculated as,

$$R_L = -qQ_\mu f_{ec} H\left(E_\mu\right) + qQ_1^L\left[1 - H\left(e_1^U\right)\right]. \tag{2}$$

In Eq. (2), q is the sifting coefficient, the subscript μ denotes the intensity of the signal state, Q_μ is the overall gain of a signal state, E_μ is the overall quantum bit error rate, Q_1^L is the lower bound of the gain of single-photon state, e_1^U is the upper bound of the error rate of a single-photon state, f_{ec} is the error correction efficiency, and $H(x)$ is the binary Shannon information function, given by $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. To calculate R_L, four key variables, Q_μ, E_μ, Q_1^L, and e_1^U, are required. The first two can be directly measured through experiments and the latter two can be estimated by the decoy state method [7].

2.4. Generic maximum-flow problem

A classical network is usually modeled as a directed graph $G = (V, E, F)$ with node set V, edge set E and *traffic-flow set* F [53], which has a communication pair $(s, t)\,(s \in V, t \in V)$ with a specific communication demand $d(s, t)$, and a positive real-valued capacity $c(u, v)$ for each edge $(u, v) \in E$.

Definition 1: A traffic-flowf on G is a non-negative function, ranging over all edges $(u, v) \in E$, satisfying the following constraints [54]:

(i) *Capacity constraint*

$$f(u, v) \le c(u, v), \forall (u, v) \in E. \tag{3}$$

(ii) *Flow conservation*

$$\sum_{v \in V} f(u, v) - \sum_{v \in V} f(v, u) = 0, \forall u \in V - \{s, t\}. \tag{4}$$

Total value of *traffic-flows*, $[\![f]\!]$, is defined as the total difference between the flows into and out of the sink t [55], i.e.,

$$[\![f]\!] = \sum_{u \in V} [f(u, t) - f(t, u)]. \tag{5}$$

The maximum-flow problem aims to compute the maximum value of $[\![f]\!]$ for a given network and it is commonly discussed in the fields of the task assignment, logistics networks, urban planning, etc.

In the context of a communication network, there are usually multiple concurrent communication pairs, in the form of calls or connections [56]. Therefore, the performance evaluation of a communication network is significantly more complicated than solving the maximum-flow problem. The classical solving algorithms for the maximum-flow problem, such as Ford-Fulkerson [57] and Edmonds-Karp [58], cannot be directly applied.

3. Flow-based mathematical model

With the increase in the coverage and complexity of existing QKD networks, it is beneficial to design an effective model for functional verification, quality assurance, cost control, cycle shortening, etc. In this section, a FM model is proposed. The "flow" does not refer to the generic *traffic-flow*, but the *QKD-flow*, which will be defined in 3.3.

By abstracting the communication party and trusted relay as nodes, the communication link as the edge, and the traffic volume as the *QKD-flow*, the definition of a QKD network is given below.

Definition 2: A QKD network is modeled as a graph $G = (V, E, F)$, where V, E, and F are the sets of nodes, edges, and QKD-flows, respectively.

3.1. Node attributes

As a communication network, the most important task of a QKD network is to satisfy the communication demand between node pairs. The concept of *connection* is used to mathematically describe the communication demand.

Optics EXPRESS

Definition 3: In the QKD network $G = (V, E, F)$, a connection$k_{ij} = \left(s_i, t_j\right)\left(s_i \in V, t_j \in V\right)$ indicates the communication demand between the node pair $\left(s_i, t_j\right)$ [59], where s_i is a source and t_j is a sink.

Let $K = \left\{\left(s_i, t_j\right) | s_i \in V, t_j \in V\right\}$ denote all the desired *connections* in the QKD network. Generally, the number of keys consumed in the communication process is determined by the communication demand and the key consumption ratio. The node attributes are illustrated in Table 1.

Table 1. Attributes of node s_i

Attributes	Symbol	Value
Communication demand	$d\left(s_i, t_j\right)$	$[0, +\infty)$
Key consumption ratio	$\beta\left(s_i, t_j\right)$	$[0, 1]$

The communication demand $d\left(s_i, t_j\right)$ is the average communication rate required by the *connection* $\left(s_i, t_j\right)$. Moreover, the communication demand of the node s_i is denoted by $d\left(s_i\right) = \left\{d\left(s_i, t_j\right) | t_j \in V\right\}$.

The key consumption ratio $\beta\left(s_i, t_j\right)$ is the ratio of the key length to the plaintext length in the adopted encryption algorithm. In particular, when the value of $\beta\left(s_i, t_j\right)$ is 1, it indicates that a One-Time-Pad (OTP) algorithm [60] was adopted to achieve secure communication. When the value of $\beta\left(s_i, t_j\right)$ is 0, it indicates that the adopted encryption algorithm does not require the keys generated by the QKD systems. The key consumption ratio of the node s_i is therefore denoted by $\beta\left(s_i\right) = \left\{\beta\left(s_i, t_j\right) | t_j \in V\right\}$.

3.2. Edge attributes

Because upstream and downstream communication share channel bandwidth [61], the edge of a QKD network is considered undirected. The undirected edge, formed by connecting nodes $u_m \in V$ and $v_n \in V$, is denoted by $(u_m, v_n) \in E$.

The main attribute of a QKD network lies in the fact that the key generation process requires the participation of a quantum channel and the key generation rate is very limited by the length of the quantum channel. In order to mathematically describe this characteristic, several important attributes of the edge are extracted. Their symbol representations and value ranges are shown in Table 2.

Table 2. Attributes of the edge (u_m, v_n)

Attributes	Symbol	Value
Classical channel capacity	$c\left(u_m, v_n\right)$	$[0, +\infty)$
Key generation capability	$r\left(u_m, v_n\right)$	$[0, +\infty)$

Classical channel capacity $c\left(u_m, v_n\right)$ represents the capability of a classical channel to transmit information. When $c\left(u_m, v_n\right)$ is 0, there is no classical channel on the edge (u_m, v_n), resulting in the infeasibility of a secure communication process.

Key generation capability $r\left(u_m, v_n\right)$ is related to the parameters of the QKD system configured on the edge (u_m, v_n). In particular, when the $c\left(u_m, v_n\right)$ is 0, there is no classical channel on the edge (u_m, v_n). Because the classical channel is required for the transmission of supplementary information during the key exchange [62], the key generation process cannot proceed on this edge. Suppose decoy state discrete-variable QKD systems are configured, according to Eq. (1),

Optics EXPRESS

the key generation capability of the edge (u_m, v_n) is calculated as,

$$r(u_m, v_n) = \begin{cases} R_{key}, & c(u_m, v_n) \neq 0 \\ 0, & c(u_m, v_n) = 0. \end{cases} \tag{6}$$

3.3. Flow conditions

Although the concept of *traffic-flow* is referred to in this paper, the flow in a QKD network has many unique features owing to the significant difference between a QKD network and generic flow network. For example, there exist many *connections* and the edge owns two types of capacities.

Definition 4: In a QKD network $G = (V, E, F)$, a QKD-flowf $\in F$ is a non-negative function ranging over all connections$(s_i, t_j) \in K$ and all edges $(u_m, v_n) \in E$, which is represented by a symbol $f(s_i, t_j, u_m, v_n)$.

Specifically, a *QKD-flow* $f(s_i, t_j, u_m, v_n)$ characterizes the net data flow from a sources s_i to a sink t_j on an edge (u_m, v_n). In other words, two *QKD-flows* are different once any of the four parameters differs, i.e. s_i, t_j, u_m and v_n.

The *QKD-flow* set F can be written as $F = \{f(s_i, t_j, u_m, v_n) \mid (s_i, t_j) \in K, (u_m, v_n) \in E\}$. Because the secure transmission process is organized in packets, the value of $f(s_i, t_j, u_m, v_n)$ must be in integer multiples of the packet size P, which is called numerical constraint and given as,

$$\frac{f(s_i, t_j, u_m, v_n)}{P} \in N, \forall (u_m, v_n) \in E, \forall (s_i, t_j) \in K, \tag{7}$$

where N is the set of all non-negative integers.

When the value of $f(s_i, t_j, u_m, v_n)$ is 0, it indicates that there is no flow of the *connection* (s_i, t_j) on the edge (u_m, v_n). In addition, the secure communication process is directed, therefore, $f(s_i, t_j, u_m, v_n)$ is considered a directed flow. Therefore, $f(s_i, t_j, u_m, v_n)$ and $f(s_i, t_j, v_n, u_m)$ are different. The special conditions of the *QKD-flow* set are analyzed below.

(i) *Capacity constraint*

- For all $(u_m, v_n) \in E$, the total flow on the edge (u_m, v_n) and its reverse edge (v_n, u_m) must be non-negative and less than or equal to its classical channel capacity. In addition, as an undirected graph, the classical channel capacity is shared by upstream and downstream flows. Thus, Eq. (8) should be satisfied.

$$\begin{aligned} 0 &\leq \sum_{(s_i, t_j) \in K} \left[f(s_i, t_j, u_m, v_n) + f(s_i, t_j, v_n, u_m) \right] \\ &\leq c(u_m, v_n), \forall (u_m, v_n) \in E. \end{aligned} \tag{8}$$

- For all $(u_m, v_n) \in E$, the total key consumption on the edge (u_m, v_n) and its reverse edge (v_n, u_m) must be non-negative and less than or equal to its key generation capability. Considering the key consumption ratio $\beta(s_i, t_j)$, the relationship between the total flow on the edge (u_m, v_n) and its reverse edge (v_n, u_m) is given by,

$$\begin{aligned} 0 &\leq \sum_{(s_i, t_j) \in K} \beta(s_i, t_j) \left[f(s_i, t_j, u_m, v_n) + f(s_i, t_j, v_n, u_m) \right] \\ &\leq r(u_m, v_n), \forall (u_m, v_n) \in E, \end{aligned} \tag{9}$$

(ii) *Flow conservation*

- For all *connections* $(s_i, t_j) \in K$ and all non-source and non-sink nodes $u_m \in V - \{s_i, t_j\}$, the total flow into the node u_m must equal to the total flow out of it, i.e.,

$$\sum_{v_n \in V} f(s_i, t_j, u_m, v_n) - \sum_{v_n \in V} f(s_i, t_j, v_n, u_m) = 0, \quad \forall u_m \neq s_i, t_j, \forall (s_i, t_j) \in K. \tag{10}$$

In general, compared to the classical network model, the distinctiveness of the FM model lies in the attributes of the key consumption ratio, key generation capability, and unique *QKD-flows*. As the theoretical foundation of topology evaluation and design, routing evaluation and design, QKD systems selection, and construction cost control, the FM model can be used not only for the construction of a new QKD network, but also for the optimization of existing QKD networks.

4. FM model based topology evaluation

To construct a high performance QKD network, designing a precise topology evaluation scheme is one of the most important tasks. An investigation on QKD network topology evaluation was conducted, based on the FM model. Firstly, the *ITS communication bound* indicator was designed to mathematically describe the quality of QKD network topology. In addition, a linear programming-based calculation algorithm is proposed to obtain the quantitative quality.

4.1. Description of topology quality

To eliminate the influence of the encryption algorithm on the topology evaluation, an OTP algorithm [60], which can provide an ITS communication service, is adopted in this section. Hence, for all $(s_i, t_j) \in K$, the value of $\beta(s_i, t_j)$ is set to 1. The quality of a QKD network topology is measured by the proposed performance indicator *ITS communication bound*.

Similar to *traffic-flow*, the total value of *QKD-flows* for a given *connection* (s_i, t_j), $[[f(s_i, t_j)]]$, is the total difference between the *QKD-flows*, which belongs to the connection (s_i, t_j), into and out of the sink t_j; this is given by,

$$[[f(s_i, t_j)]] = \sum_{u_m \in V, v_n = t_j} \left[f(s_i, t_j, u_m, v_n) - f(s_i, t_j, v_n, u_m)\right]. \tag{11}$$

Let $M(s_i, t_j)$ represent the satisfaction degree of communication demand, that is, the so-called *satisfactory-degree*, for a given *connection* (s_i, t_j), which is the ratio of its total value to its communication demand, i.e.,

$$M(s_i, t_j) = \frac{[[f(s_i, t_j)]]}{d(s_i, t_j)}. \tag{12}$$

Here, $M(s_i, t_j) \geq 1$ indicates that the communication demand of the connection (s_i, t_j) is satisfied.

Because there are multiple *connections* [30] in a QKD network, the performance of the entire network for a given *QKD-flow* assignment F, which is indicated by $\rho(F)$, can be represented by the worst performance of all *connections*. Therefore, we can calculate all the *satisfactory-degrees* for all *connections* and then obtain the minimum value, *min-satisfactory-degree*. Obviously, each possible *QKD-flow* assignment corresponds to a specific *min-satisfactory-degree*, which can be calculated as,

$$\rho(F) = \min_{(s_i, t_j) \in K} M(s_i, t_j). \tag{13}$$

Similar to the generic maximum-flow problem, we can obtain the optimization (maximum) of all possible *min-satisfactory-degrees* through the optimal assignment of *QKD-flows*. This maximum value, which is called *ITS communication bound*, can be used to represent the optimal performance of a QKD network with a given topology.

Optics EXPRESS

Definition 5: For a QKD network with a given topology, the ITS communication bound is defined as the optimization (maximum) of all possible min-satisfactory-degrees, each of which is defined as the minimum of all satisfactory-degrees for all connections in K over a possible QKD-flow assignment.

The *ITS communication bound B* is therefore can be calculated as,

$$B = \max_F \rho(F), \tag{14}$$

It is clear that the communication demand for all *connections* is satisfied only when the value of B is greater than 1. The larger the value of B, the higher the degree of satisfaction. It is also significant that, for a specific QKD network with specific routing protocols and specific key management strategies, the gap between running performance and the calculation of *ITS communication bound* can be used to evaluate the performance of the routing protocols and key management strategies.

4.2. Calculation of topology quality

To calculate the indicator B, it is necessary to explore the optimal assignment of the *QKD-flows*, which is defined as the multi-connection flow problem (MCFP) in this paper. Although the MCFP appears to be a combination of several maximum-flow problems, the interaction of multiple maximum-flow problems cause their respective solutions to fail [63].

With regard to the definition of a *QKD-flow*, the flow must satisfy the capacity constraint and flow conservation. Therefore, the MCFP can be formulated as,

$$\max_F \quad \min_{(s_i,t_j)\in K} \frac{\sum_{u_m\in V, v_n=t_j} \left[f\left(s_i,t_j,u_m,v_n\right) - f\left(s_i,t_j,v_n,u_m\right)\right]}{d\left(s_i,t_j\right)}, \tag{15a}$$

$$\text{s.t.} \quad \text{Eq. (7)}, \text{Eq. (8)}, \text{Eq. (9)}, \text{Eq. (10)}. \tag{15b}$$

In Eq. (15), $F = \left\{f\left(s_i,t_j,u_m,v_n\right) \mid \left(s_i,t_j\right)\in K, \left(u_m,v_n\right)\in E\right\}$ are the set of decision variables. The formulation is very similar to that of the linear programming problem. However, due to the issues of a non-linear objective function and the non-standard data type of the decision variables, the MCFP is not a standard linear programming problem, which is difficult to solve. To transform this problem into standard linear programming, the original decision variable $f\left(s_i,t_j,u_m,v_n\right)$ must be converted into a new variable $x\left(s_i,t_j,u_m,v_n\right)$ as follows:

$$x\left(s_i,t_j,u_m,v_n\right) = \frac{f\left(s_i,t_j,u_m,v_n\right)}{P}. \tag{16}$$

Therefore, $X = \left\{x\left(s_i,t_j,u_m,v_n\right) \mid \left(s_i,t_j\right)\in K, \left(u_m,v_n\right)\in E\right\}$ becomes the new set of decision variables. In addition, the original objective function is replace by a new objective function $\rho(F)$, by adding $\rho(F)$ as a new decision variable and adding two constraint conditions, as follows,

$$\frac{\rho(F)}{P} - \frac{\sum_{u_m\in V, v_n=t_j} \left[x\left(s_i,t_j,u_m,v_n\right) - x\left(s_i,t_j,v_n,u_m\right)\right]}{d\left(s_i,t_j\right)} \le 0, \forall\left(s_i,t_j\right)\in K, \tag{17a}$$

$$\rho(F)\in R_0^+, \tag{17b}$$

where R_0^+ is the set of non-negative real numbers.

According to the above operations, the MCFP is transformed into an equivalent standard mixed integer linear-programming problem, which is formulated as:

$$\max_{X} \quad \rho(F) \tag{18a}$$

$$\text{s.t.} \quad 0 \le \sum_{(s_i,t_j)\in K} x\left(s_i,t_j,u_m,v_n\right) + \sum_{(s_i,t_j)\in K} x\left(s_i,t_j,v_n,u_m\right) \le \frac{c\left(u_m,v_n\right)}{P}, \forall\left(u_m,v_n\right)\in E, \tag{18b}$$

$$0 \le \sum_{(s_i,t_j)\in K} x\left(s_i,t_j,u_m,v_n\right) + \sum_{(s_i,t_j)\in K} x\left(s_i,t_j,v_n,u_m\right) \le \frac{r\left(u_m,v_n\right)}{P}, \forall\left(u_m,v_n\right)\in E, \tag{18c}$$

$$\sum_{v_n\in V} x\left(s_i,t_j,u_m,v_n\right) - \sum_{v_n\in V} x\left(s_i,t_j,v_n,u_m\right) = 0, \forall u_m \ne s_i,t_j, \forall\left(s_i,t_j\right)\in K, \tag{18d}$$

$$\frac{\rho(F)}{P} - \frac{\sum\limits_{u_m\in V, v_n=t_j}\left[x\left(s_i,t_j,u_m,v_n\right) - x\left(s_i,t_j,v_n,u_m\right)\right]}{d\left(s_i,t_j\right)} \le 0, \forall\left(s_i,t_j\right)\in K, \tag{18e}$$

$$x\left(s_i,t_j,u_m,v_n\right)\in N, \forall\left(u_m,v_n\right)\in E, \forall\left(s_i,t_j\right)\in K, \tag{18f}$$

$$\rho(F)\in R_0^+. \tag{18g}$$

In order to solve this problem, a linear programming solver [64], Gurobi [65], was adopted. In the formulation, $r\left(u_m,v_n\right)$ represents the key generation capability of a QKD system. It is important to note that many types of QKD systems can be adopted into the QKD network and the corresponding topology quality can be obtained by changing the calculation of $r\left(u_m,v_n\right)$.

5. Simulation results and analysis

5.1. Simulation design

The design of this simulation consisted mainly of the design of the parameters for communication demand, QKD systems, packet size, and classical channel capacities. These parameters will directly affect the topology performance of a specific QKD network. During the simulation, typical topologies of the SECOQC and NSFNET network were adopted.

To simplify the analysis, the communication demand between any two different nodes in the simulation was assumed to be the same, denoted as d, i.e.,

$$K = \left\{\left(s_i,t_j\right) | s_i\in V, t_j\in V, s_i\ne t_j\right\}, \tag{19a}$$

$$d\left(s_i,t_j\right) = \begin{cases} d, \left(s_i,t_j\right)\in K, \\ 0, \left(s_i,t_j\right)\notin K. \end{cases} \tag{19b}$$

Given that the discrete-variable QKD protocol is one of the most practical QKD protocols and that the decoy state method is critical to security assurance, a decoy state discrete-variable QKD system was adopted in this simulation. To simplify analysis, the parameters of all QKD systems were assumed to be the same. To facilitate a comparison with the performance reported in the literature [7], the same parameters of QKD system, listed in Table 3, and the same packet size, that is, $P = 500$ bytes, were adopted in this simulation.

In Table 3, f_{req} is the repetition rate, q is the sifting coefficient, α is the fiber attenuation coefficient, η_{Bob} is the transmittance of Bob, e_{det} is the intrinsic error rate due to misalignment and instability of the optical system, μ is the intensity of signal state, ν is the intensity of decoy state, ϕ is the intensity of vacuum state, Y_0 is the background rate, e_0 is the error rate of the

Optics EXPRESS

Table 3. Parameters of QKD systems [7]

f_{req}	q	α	η_{Bob}	e_{det}	μ	ν	ϕ	Y_0	e_0	f_{ec}	N_μ	N_ν	N_ϕ	ς
1GHz	0.9	0.2dB/km	0.1	0.01	0.4	0.1	0	2.1E-5	0.5	1.15	1.6E10	2E9	2E9	5.73E-7

background, f_{ec} is the error correction efficiency, N_μ is the number of signal pluses sent by Alice, N_ν is the number of decoy pluses sent by Alice, N_ϕ is the number of vacuum pluses sent by Alice, ς is the security bound.

Because classical optical fiber communication technology is sufficiently mature [66,67], the classical channel capacities of all the edges were set to 1 Gbps, i.e.,

$$c(u_m, v_n) = 1 \text{ Gbps}, \forall (u_m, v_n) \in E. \tag{20}$$

5.2. Topology evaluation based on QKD system placement

A typical task undertaken as part of network topology planning involves investigating how to effectively enhance the network performance by adding just one system to existing topology. In the context of a QKD network, the equivalent task involves finding out how to effectively enhance the QKD network performance by adding a QKD system to an existing QKD network topology. When the new QKD system is added, which is equivalent to adding a new edge to existing topology, a modified topology is actually formed.

It is well known that the key generation process is reliant on the optical fiber. Therefore, a QKD system can function only when placed on the existing edge. In addition, adding a QKD system to the edge (u_m, v_n) results in an increase in the key generation capability of this edge and its reverse edge, $r(u_m, v_n)$ and $r(v_n, u_m)$. Due to the different link distances, the key generation capabilities of a given QKD system will vary depending on the edge on which it is placed. In addition, due to the different traffic burdens of edges within the overall network, any given QKD system will produce different gains in communication security depending on the edge on which it is placed.

To verify validity of the proposed FM model and performance indicator, a network topology of the SECOQC network, which is shown in Fig. 2, was selected. The numbers on the edges in the figure represent the link distances in kilometers. To determine the optimal placement scheme, the QKD system is placed at every possible edge in a SECOQC network, to form eight modified topologies. To quantitatively evaluate different placement schemes, the *ITS communication bounds* of the original SECOQC topology and the eight modified SECOQC topologies were calculated. The results are listed in Table 4.

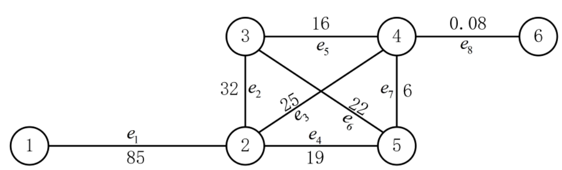


Fig. 2. Topology of SECOQC network [7]

Table 4. Performance comparison of original SECOQC topology and modified SECOQC topologies (d = 25 Kbps)

Placement	*none*	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8
Bound	0.96	1.92	0.96	0.96	0.96	0.96	0.96	0.96	0.96

Table 4 shows that the *ITS communication bound* increased and the communication demand switched from unsatisfied to satisfied when the QKD system was placed on edge e_1. This indicates that edge e_1 acts as a bottleneck in the topology of the SECOQC network, which is consistent with the performance results in the literature [7].

If we observe the original SECOQC topology in Fig. 2, we can see that the length of edge e_1 is 85 km. By substituting this length into Eq. (2), the calculated key generation capability is approximately 233 Kbps. However, as a "bridge" [68] in the topology, no matter which routing algorithm is adopted, the keys generated on edge e_1 must satisfy the communication demand for ten connections (s_1, t_2), (s_1, t_3), (s_1, t_4), (s_1, t_5), (s_1, t_6), (s_2, t_1), (s_3, t_1), (s_4, t_1), (s_5, t_1), and (s_6, t_1) . Thus, when the communication demand is set to 25 Kbps, the *ITS communication bound* can be calculated as $233/(25*10) \approx 0.93$. In addition, when the addition QKD system is placed on the edge e_1, the modified *ITS communication bound* can be calculated as $(233*2)/(25*10) \approx 1.86$. The alignment between this calculation and the result shown in Table 4 is due to the numerical constraint of *QKD-flows*.

It is clear that the distances corresponding to the other edges are significantly shorter than edge e_1, which is conducive to a higher key generation capability. As the traffic burden is eased, only one QKD system placed on these edges will not exhibit a more significant performance improvement. The validity of FM model and *ITS communication bound* indicator is verified.

5.3. Topology evaluation based on intermediate node selection

Although the above mentioned results are quite sufficient for the demonstration of the validity of the research, another simulation based on intermediate node selection was designed to further verify the necessity of the proposed model and indicator.

Node selection, i.e., the effective enhancement of network performance by adding several intermediate nodes and corresponding edges to an existing topology, is also a typical task in network topology planning. Because a QKD network based on the trusted relay mode requires every node in the topology to be trusted, the addition of a new node will reduce the security of this QKD network. Therefore, compared with a classical network, node selection is more important for a QKD network.

To verify the necessity of the proposed FM model and performance indicator, a complicated topology of the NSFNET network, which is shown in Fig. 3, was designed. The three gray nodes in Fig. 3 are optional nodes with no communication demand. In contrast, every pair of other nodes has the same communication demand. A dotted line in the figure represents an optional edge that connects one or two optional nodes. To simplify the analysis, this simulation assumed that an optional edge is selected if and only if the nodes at both ends of this edge are selected. In addition, the same parameters for communication demand, QKD system, packet size, and classical channel capacities were adopted.

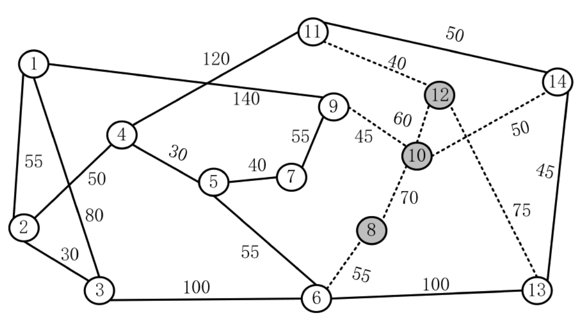
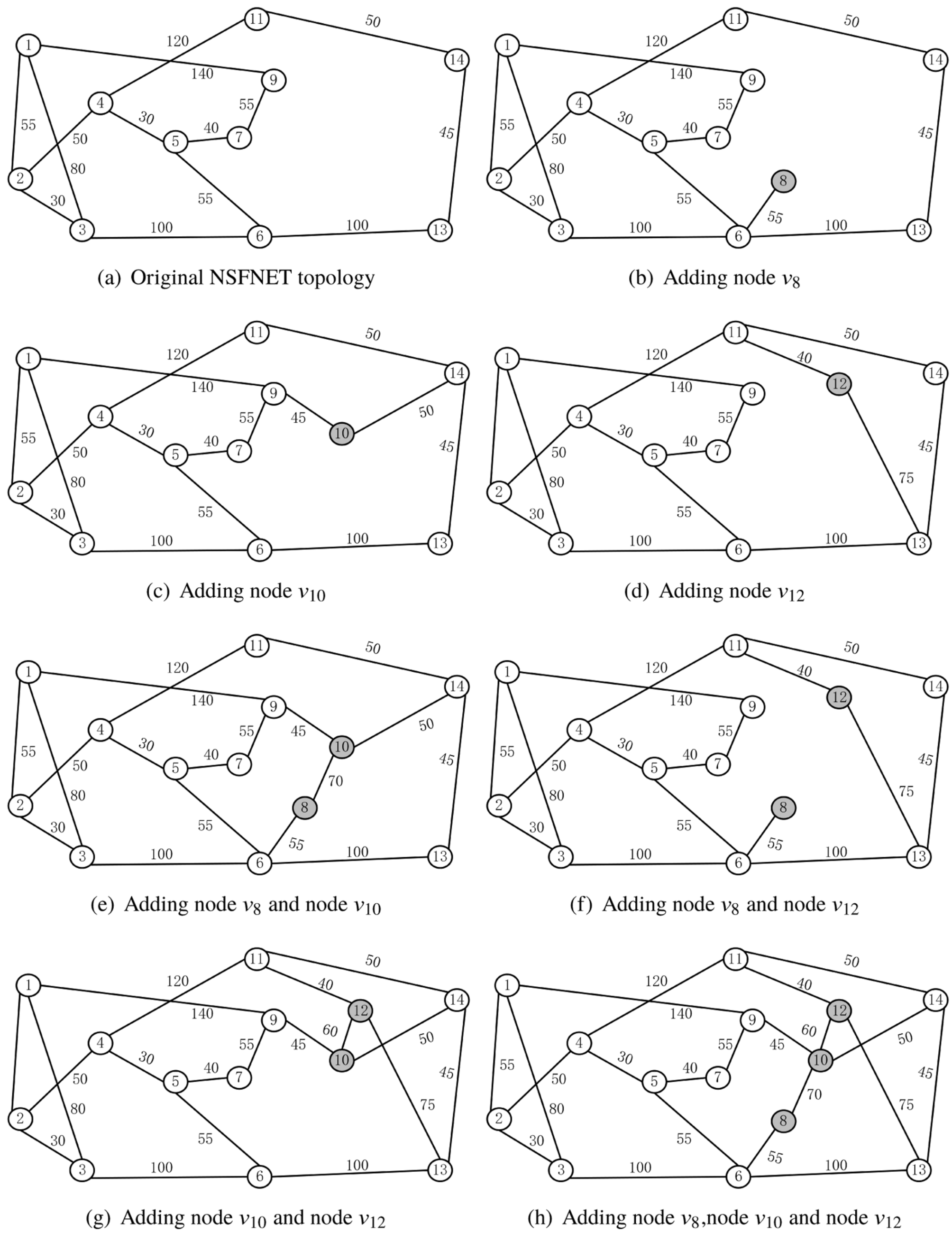


Fig. 3. Topology of NSFNET network

Optics EXPRESS

To determine the optimal selection scheme, different combinations of the three optional nodes were used, which form eight different topologies as shown in Fig. 4. To quantitatively evaluate different selection schemes, the *ITS communication bounds* under these eight different topologies were calculated. The results are listed in Table 5.



(a) Original NSFNET topology
(b) Adding node v_8
(c) Adding node v_{10}
(d) Adding node v_{12}
(e) Adding node v_8 and node v_{10}
(f) Adding node v_8 and node v_{12}
(g) Adding node v_{10} and node v_{12}
(h) Adding node v_8,node v_{10} and node v_{12}

Fig. 4. Eight different topologies

For ease of presentation, we use Bound(X) to denote the value of *ITS communication bound* when the selection is X. As listed in Table 5, Bound(v_{10}) > 1 and Bound(v_8) = Bound(v_{12}) =

Table 5. Performance comparison under the eight different topologies (d = 15 Kbps)

Selection	*none*	v_8	v_{10}	v_{12}	v_8, v_{10}	v_8, v_{12}	v_{10}, v_{12}	*all*
Bound	0.104	0.104	1.642	0.104	2.352	0.104	1.642	2.352

Bound(*none*) < 1. Therefore, to meet the communication demand, the addition of the single node v_{10} gives the best selection. In contrast, adding the node v_8 or v_{12} does not yield any gain in performance. In addition, Bound(v_8, v_{10}) > Bound(v_{10}); i.e., on the basis of adding node v_{10}, adding node v_8 will result in more gains in performance. However, Bound(v_{12}, v_{10}) = Bound (v_{10}), Bound(v_{12}, v_8) = Bound (v_8) and Bound(*all*) = Bound(v_8, v_{10}). Therefore, in any case, the addition of node v_{12} does not bring any gain in performance.

In general,the communication demand can be met by adding only node v_{10}. On this basis, adding node v_8 will further enhance the performance of the entire network. However, the addition of node v_{12} does not offer any gain in performance. This conclusion cannot be intuitively inferred; therefore, the necessity of the proposed FM model and *ITS communication bound* indicator is verified.

6. Conclusion

This paper has proposed a flow-based mathematical model of a QKD network. The major contributions of this study include: (I) The FM model was proposed by modeling a QKD network as a graph with nodes, edges, and *QKD-flows*; (II) Based on the created model, a unique QKD network performance indicator was proposed and the corresponding linear programming-based calculation algorithm was designed; (III) The validity and necessity of the proposed FM model and performance indicator were verified through subtly designed simulations addressing two typical topology evaluation tasks. This study provide us with the means to explore new possibilities in the area of QKD networking and promote the development of QKD networking technology.

The FM model proposed in this paper can be used for the networking of all kinds of point-to-point QKD protocols, such as the BB84-QKD protocol, decoy-QKD protocol, and GG02-QKD protocol. However, some QKD protocols that need to set up a third party, such as MDI-QKD protocol and TF-QKD protocol, cannot be supported. In the future, we will continue to study the networking of such non-point-to-point QKD protocols. In addition, a decoy state discrete-variable QKD protocol was selected in the simulation of this paper. However, it is well known that there are many kinds of QKD protocols that have been put to practical use. In the process of network construction, to control the construction cost, it is necessary to select a reasonable QKD protocol according to the specific application. The FM model can be used to guide the selection of QKD systems by accurately calculating the network topology performance when parameters are set. However, the iterative method for network construction is not sufficiently efficient because it incurs a selection process ultimately leading to the selection of the best case. In our future research, it will be necessary to further consider the relationship between the QKD protocol, link distance, topology, and other factors to propose an efficient and adaptive construction scheme.

Funding

Space Science and Technology Advance Research Joint Funds (6141B06110105); National Natural Science Foundation of China (61771168).

Disclosures

The authors declare no conflicts of interest.

References

1. 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. Rev. Lett. **117**(19), 190501 (2016).
2. 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**(7670), 43–47 (2017).
3. 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. Lightwave Technol. **36**(16), 3427–3433 (2018).
4. 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**(3), 035006 (2019).
5. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Theor. Comput. Sci. **560**, 7–11 (2014).
6. M. F. Tüysüz and H. A. Mantar, "A local estimation of node quantity and channel density for voip applications over ieee 802.11 e wlans," in *ICIMU 2011: Proceedings of the 5th international Conference on Information Technology & Multimedia*, (IEEE, 2011), pp. 1–5.
7. Y. Wang, Q. Li, Q. Han, and Y. Wang, "Modeling and simulation of practical quantum secure communication network," Quantum Inf. Process. **18**(9), 278 (2019).
8. 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.
9. C. Elliott and H. Yeh, "Darpa quantum network testbed," Tech. rep., BBN TECHNOLOGIES CAMBRIDGE MA (2007).
10. A. Poppe, M. Peev, and O. Maurhart, "Outline of the secoqc quantum-key-distribution network in vienna," Int. J. Quantum Inf. **06**(02), 209–218 (2008).
11. R. Alleaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, "Topological optimization of quantum key distribution networks," New J. Phys. **11**(7), 075002 (2009).
12. 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.
13. 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. Rev. Lett. **120**(3), 030501 (2018).
14. 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**(11), 10387–10409 (2011).
15. M. Razavi, *An Introduction to Quantum Communications Networks*, 2053–2571 (Morgan & Claypool Publishers, 2018).
16. 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**(7), 075001 (2009).
17. M. Dianati, R. Alléaume, M. Gagnaire, and X. Shen, "Architecture and protocols of the future european quantum key distribution network," Secur. Commun. Networks **1**(1), 57–74 (2008).
18. E. Diamanti, H. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Inf. **2**(1), 16025 (2016).
19. 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).
20. 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 Multimedia Signal Process. **5**(1), 13–19 (2014).
21. N. Mahmud, E. Elaraby, and D. Caliga, "Scaling reconfigurable emulation of quantum algorithms at high-precision and high-throughput," Quantum Eng. **1**(2), e19 (2019).
22. C. Yang, H. Zhang, and J. Su, "The qkd network: model and routing scheme," J. Mod. Opt. **64**(21), 2350–2362 (2017).
23. 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**(10), 253 (2017).
24. T. R. Henderson, M. Lacage, G. F. Riley, C. Dowell, and J. Kopena, "Network simulations with the ns-3 simulator," SIGCOMM demonstration **14**, 527 (2008).
25. D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, (IEEE, 2004), p. 136.
26. P. K. Tysowski, X. Ling, N. Lütkenhaus, and M. Mosca, "The engineering of a scalable multi-site communications system utilizing quantum key distribution (qkd)," Quantum Sci. Technol. **3**, 024001 (2018).
27. A. Aguado, V. Lopez, D. Lopez, M. Peev, A. Poppe, A. Pastor, J. Folgueira, and V. Martin, "The engineering of software-defined quantum key distribution networks," IEEE Commun. Mag. **57**(7), 20–26 (2019).
28. H. Wang, Y. Zhao, and A. Nag, "Quantum-key-distribution (qkd) networks enabled by software-defined networks (sdn)," Appl. Sci. **9**(10), 2081 (2019).

Optics EXPRESS

29. D. Huang, Y. Zhao, T. Yang, S. Rahman, X. Yu, X. He, and J. Zhang, "Quantum key distribution over double-layer quantum satellite networks," IEEE Access **8**, 16087–16098 (2020).
30. H. Zhou, K. Lv, L. Huang, and X. Ma, "Security assessment and key management in a quantum network," arXiv preprint arXiv:1907.08963 (2019).
31. 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. **57**(5), 152–159 (2019).
32. 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 **27**(3), 2544–2561 (2019).
33. A. Schrijver, "On the history of the transportation and maximum flow problems," Math. Program. **91**(3), 437–445 (2002).
34. S. Han, Z. Peng, and S. Wang, "The maximum flow problem of uncertain network," Inf. Sci. **265**, 167–175 (2014).
35. K. L. Calvert, M. B. Doar, and E. W. Zegura, "Modeling internet topology," IEEE Commun. Mag. **35**(6), 160–163 (1997).
36. P. Yi and B. Ramamurthy, "Provisioning virtualized cloud services in ip/mpls-over-eon networks," Photonic Netw. Commun. **31**(3), 418–431 (2016).
37. P. D. Townsend, "Quantum cryptography on multiuser optical fibre networks," Nature **385**(6611), 47–49 (1997).
38. 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 Technol. **23**(1), 268–276 (2005).
39. 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.
40. 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**(11), 1669–1671 (2003).
41. 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**(11), 695–699 (2017).
42. 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**(2), e13 (2019).
43. M. Dianati and R. Alléaume, "Architecture of the secoqc quantum key distribution network," in *Quantum, Nano, and Micro Technologies, 2007. ICQNM'07. First International Conference on*, (IEEE, 2007), pp. 13.
44. C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, (ACM, 2002), pp. 80–91.
45. Q. Li, X. Wen, H. Mao, and X. Wen, "An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution," Quantum Inf. Process. **18**(1), 25 (2019).
46. H. Mao, Q. Li, Q. Han, and H. Guo, "High-throughput and low-cost ldpc reconciliation for quantum key distribution," Quantum Inf. Process. **18**(7), 232 (2019).
47. Q. Li, B. Yan, H. Mao, X. Xue, Q. Han, and H. Guo, "High-speed and adaptive fpga-based privacy amplification in quantum key distribution," IEEE Access **7**, 21482–21490 (2019).
48. Q. Li, Q. Zhao, D. Le, and X. Niu, "Study on the security of the authentication scheme with key recycling in qkd," Quantum Inf. Process. **15**(9), 3815–3831 (2016).
49. A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," Phys. Rev. Lett. **114**(7), 070501 (2015).
50. M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," Nat. Commun. **5**(1), 3732 (2014).
51. X. Ma, B. Qi, Y. Zhao, and H. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**(1), 012326 (2005).
52. X. Ma, C. F. Fung, and M. Razavi, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution," Phys. Rev. A **86**(5), 052305 (2012).
53. A. V. Goldberg, É. Tardos, and R. E. Tarjan, "Network flow algorithms," Tech. rep., PRINCETON UNIV NJ DEPT OF COMPUTER SCIENCE (1989).
54. T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms* (MIT press, 2009).
55. A. V. Goldberg and R. E. Tarjan, "A new approach to the maximum-flow problem," J. Assoc. Comput. Mach. **35**(4), 921–940 (1988).
56. N. Brownlee, C. Mills, and G. Ruth, "Rfc 2722: Traffic flow measurement: Architecture," IETF, Tech. Rep. (1999).
57. L. R. Ford and D. R. Fulkerson, "Maximal flow through a network," in *Classic papers in combinatorics*, (Springer, 2009), pp. 243–248.
58. J. Edmonds and R. M. Karp, "Theoretical improvements in algorithmic efficiency for network flow problems," J. Assoc. Comput. Mach. **19**(2), 248–264 (1972).
59. K. Cai and P. Fan, "Link decomposition of network coding," in *2006 Asia-Pacific Conference on Communications*, (IEEE, 2006), pp. 1–5.
60. S. Watanabe, R. Matsumoto, and T. Uyematsu, "Security of quantum key distribution protocol with two-way classical communication assisted by one-time pad encryption," arXiv preprint quant-ph/0608030 (2006).

Optics EXPRESS

61. B. Sklar and F. J. Harris, *Digital communications: fundamentals and applications*, vol. 2001 (Prentice-hall Englewood Cliffs, NJ, 1988).
62. Q. Li, D. Le, X. Wu, X. Niu, and H. Guo, "Efficient bit sifting scheme of post-processing in quantum key distribution," Quantum Inf. Process. **14**(10), 3785–3811 (2015).
63. W. Dai, X. Sun, and S. Wandelt, "Finding feasible solutions for multi-commodity flow problems," in *2016 35th Chinese Control Conference (CCC)*, (IEEE, 2016), pp. 2878–2883.
64. B. Meindl and M. Templ, "Analysis of commercial and free and open source solvers for linear optimization problems," Eurostat. Stat. Neth. within project ESSnet on common tools harmonised methodology for SDC ESS **20** (2012).
65. G. Optimization, "Inc., 'gurobi optimizer reference manual,' 2015," (2014).
66. J. Hecht, "Ultrafast fibre optics set new speed record," New Sci. **210**(2809), 24 (2011).
67. W. Idler, F. Buchali, L. Schmalen, E. Lach, R. Braun, G. Böcherer, P. Schulte, and F. Steiner, "Field trial of a 1 tb/s super-channel network using probabilistically shaped constellations," J. Lightwave Technol. **35**(8), 1399–1406 (2017).
68. J. A. McHugh, *Algorithmic graph theory*, vol. 68056 (Prentice Hall Englewood Cliffs, NJ, 1990).