Incremental Deployment for a QKD Network

Luyao Luo Gongming Zhao

***Abstract*—**
***Index Terms*—Quantum Network.**

I. Introduction

Secure information exchange via quantum networks has been proposed, studied, and validated since 1980s [5, 17, 18, 34, 37, 47, 58] and many experimental studies have demonstrated that long-distance secrete sharing via quantum networks can become successful in reality, such as the DARPA quantum network [18], SECOQC Vienna QKD network [37], the Tokyo QKD network [47], and the satellite quantum network in China [58]. A quantum network (also called a quantum Internet) is an interconnection of quantum processors and repeaters that can generate, exchange, and process quantum information [8, 10, 24, 56]. It transmits information in the form of quantum bits, called qubits, and stores qubits in quantum memories. Quantum networks are not meant to replace the classical Internet communication. In fact, they supplement the classical Internet and enable a number of important applications such as quantum key distribution (QKD) [5, 17, 40], clock synchronization [25], secure remote computation [7], and distributed consensus [15], most of which cannot be easily achieved by the classical Internet.

With the help of quantum key distribution, it supports highly secure communication between two terminals. With this significant advantage, many users, including corporations and governments, are expecting to deploy a QKD network. As there has already deployed a traditional data communication network, a primary task for applying a QKD network is how to efficiently deploy a QKD network while integrating with the current data network. To be compatible with the traditional data network, we will deploy a set of quantum relay devices and configure a certain number of qubits on each relay. When users expect to deploy a QKD network, they should consider the following factors and constraints:

1) Since QKD network just provides quantum key for communication, it should be applied with data networks. As a result, the deployment of QKD networks should be integrated with the deployment of traditional networks.
2) With a limited budget, users may ask to deploy a small number of trusted quantum relays and activate a small number of qubits, so that each pair can transmit the data with required quantum key.
3) Traffic dynamic is a common and important issue in a network.

These practical factors and constraints bring some challenges for designing an efficient QKD network. As deployment is an important issue for application of a QKD network, some studies [12] [13] have focused on this problem recently.

After deployment of QKD devices, it is another critical task to design an efficient routing mechanism in the newly deployed network.

This paper focuses on how to efficiently deploy a QKD network while considering all the above factors and constraints. We study the incremental deployment strategy, which will preserve the benefits of legacy systems. To make this possible, we address two critical technical challenges: the incremental deployment and multi-commodity flow routing in a network.

The rest of this paper is organized as follows. Section 2 discusses the related works on the deployment and routing problems under the QKD network paradigm. Section 3 gives some preliminaries. In section 4, we define the incremental deployment problem, and propose an approximate algorithm to deal with this challenge. The experimental results are presented in Section 6. We conclude the paper in Section 7.

II. Preliminaries

A. QKD Network Topology Model

In QKD network we mainly consider two kinds of deployment: quantum relay depolyment and quantum device depolyment. That is, how to choose proper locations to establish relays and how to place enough quantum devices to satisfy endpoints communication requirements. Let $N = \{n_1, n_2, ..., n_m\}$ represent the QKD endpoint set, where $m = |N|$ is the number of endpoints. $Q = \{q_1, q_2, ..., q_k\}$ represents the relay set, where $k = |Q|$ is the number of relays. Let y_{n_i} and y_{q_j} denote the number of quantum devices in endpoint n_i and relay q_j. And E denotes the set of link, such as optical fibers, between endpoints and relays. We perform QKD between two nodes(endpoints or relays) through a quantum channel built on a physical link of E.

To achieve the security requirements of relays, we can not choose random places to deploy relays in practice. Based on the existing traditional network topology, the locations of relays can coincide with some key locations(such as core switches) in a candidate location set, which is denoted as $P = \{p_1, p_2, ..., p_s\}$, with $s = |P|$. That's to say, relay set Q is a subset of candidate location set P, and each pair of endpoints can perform QKD through some relays in Q with quantum channel length constraint satisfied.

B. Problem Statement

In this section, we propose the problem statement of QKD network topology control (QNTC). Under the metropolitan area network, some organizations will deploy some quantum key distribution endpoints(QKD Endpoint) for secure communications and each pair of endpoints may have QKD requirement. Direct communication may be not supported because QKD endpoints can be far apart, so we need to deploy some trusted QKD relays to implement quantum key distribution. To achieve the security requirements of trusted relays, we can not choose random places to deploy relays. Based on the existing traditional network topology, the locations of trusted relays can coincide with some key locations(such as core switches) in a candidate location set P. QKD network topology control(QNTC) relies on the deployment of trusted relays and optical fibers to connect these QKD endpoints.

We assume that each endpoint pair needs at least one quantum channel, so there must be at least one available path for each endpoint pair that satisfies quantum constraints. There are mainly two constraints. One is the quantum resource capacity of a relay, which leads to the limited number of quantum channels passing through this relay. The other one is the link length constraint, that is, the length of any link must not exceed a given threshold, otherwise the quantum signals will not be measured correctly.

Considering the high price of quantum devices, we want to deploy as few devices as possible. However, due to the concurrency requirement(that is, the set of paths are contention-free while all the S-D pairs communicate at the same time), the number of quantum devices in each relay should be enough to satisfy the path width requirement for each pair.

The QNTC problem decides how to choose candidate positions to deploy quantum relays and how to deploy quantum devices in each relay. and our goal is to reduce the network deployment cost.

III. QKD Network Deployment

This section first defines the problem of quantum network topology Control(QNTC) and then gives an approximation algorithm to solve this problem.

A. Problem Definition for QNTC

In this section, we give the problem definition for QKD network topology control (QNTC). We assume that the cost for each quantum relay is denoted as α and the cost for quantum devices for each quantum channel passing through each relay is denoted as β. Our goal is to minimum the total cost while deploying the whole QKD network, which is consist of the cost for relays and the cost for devices.

We use x_i to denote that whether to deploy relay at position $p_i \in P$ ($x_i = 1$) or not ($x_i = 0$). And y_i denotes the number of quantum channel passing through position $p_i \in P$. Since there should be at least one quantum channel between each S-D pair, there must be at least one available path(includes relays and endpoints) where the physical length of each link is less than L_{max}. For any S-D pair f, we can find all the candidate paths that satisfy the link length constraint, denoted as T_f. z_j^f denotes that if we use the candidate path t_j^f chosen from T_f or not. w_f denotes the quantum bandwidth(or the number of qubit) required by S-D pair f and v_f denotes the data bandwidth required by f. $c(e)$ presents the traffic capacity of link e.

$$\min \quad \alpha \sum_{p \in P} x_p + \beta \sum_{p \in P} y_p$$

$$S.t. \begin{cases} \sum_{t \in T_f} z_f^t = 1, & \forall f \in F \\ z_f^t \le x_p, & \forall p \in t, \forall t \in T_f, \forall f \in F \\ \sum_{f \in F} \sum_{p \in t : t \in T_f} z_f^t \cdot w_f \le y_p, & \forall p \in P \\ \sum_{f \in F} \sum_{e \in t : t \in T_f} z_f^t \cdot v_f \le c(e), & \forall e \in E \\ x_i \in \{0, 1\} \\ y_i \in \{1, 2, ...\} \\ z_f^t \in \{0, 1\} \end{cases} \tag{1}$$

The first set of equalities denotes each S-D pair f should select one path for quantum key distribution. The second set of inequalities means if a S-D pair f chooses a path t_j^f, then all the positions on this path should deploy a relay(x_i = 1). The third set of inequalities indicates at most y_i quantum channels can pass through p_i. The fourth set of inequalities presents the traffic load on each link e should not exceed c(e).

To find candidate path set T_f for each f, firstly we construct a graph with given node set consists of endpoint set N and candidate location set P. Then we add a link between any two nodes if the physical length of link between them is less than L_{max}. After construction, we can run an algorithm(such as Yen's [1]) on this graph to get multiple paths T_f for each S-D pair f.

Theorem 1: The quantum key distribution network control problem is NP-hard.

We can prove that the typical Steiner Minimum Tree with Minimum Steriner Point(SMT-STP) problem is a special case of our problem. Considering each pair of endpoints as a S-D pair and ignoring the quantum device cost, our problem becomes a steiner minimun tree with minimum steiner point problem. Since such a problem is NP-hard, our problem is NP-hard.

B. Problem Complexity Analysis

The QNTC problem remains challenging even when some constraints are relaxed as mentioned before. We will introduce some special cases in literature to show the universality of our problem.

Steiner Minimum Tree with Minimum Steriner Point with length constraints problem: Given a network topology G={D,E} and a set of point S, we use as few points as possible in point set D so that every point in S is connected.

Shortest Path Selection problem: Given a network topology G={D,E}, and a set of S-D pair F, we explore the

shortest path for each $f \in F$. In this problem, we use hops to present the length of each path.

The main difference from the above two problem to our problem is that our problem is a joint problem of point selection and path selection. However, in steiner minimum tree problem, we only require one available path each S-D pair and in shortest path selection problem, we only search for the shortest path to use as less devices as possible. Typical algorithms for SMT never consider the path lengths for S-D pairs. But in our problem, the path length impacts the number of devices used, so we need to consider both relay selection and path selection at the same time.

This suggests that the QNTC problem is substantially harder than the SMT-MSP problem described above, and thus a different method is needed to find a tight approximation ratio. In the next section, we present a method with approximation performance guarantees.

C. Rounding-Based Deployment Algorithm for QKD Network

In this section, we propose a rounding-based deployment algorithm for the QKD network topology control problem, described in Alg.**??**. Due to the difficulty of the QNTC problem, the first step obtains the fractional solution for the relaxed QNTC problem. In the second step, we choose one feasible path for each S-D pair using randomized rounding method. Finally. we deploy both relays and devices of all candidate positions based on the paths we choose.

Algorithm 1 RQTC:Rounding-based QKD Network Topology Control

Step 1: Solving the Relaxed QNTC Problem
Construct a linear optimization program in Eq.8
Obtain the optimal solutions $\widetilde{z}_f^t$
Step 2: Selecting Paths for S-D pairs
Derive an integer solution $\hat{z_f^t}$ by randomized rounding
for each S-D pair $f \in F$ **do**
  for each feasible path $t \in T_f$ **do**
    if $\hat{z_f^t} = 1$ **then**
      Appoint a feasible path t for S-D pair f
Select quantum relays and deploy quantum devices according to path selection

In the first step, the algorithm constructs the relaxed linear problem of Eq.1, and solves the relaxed program Eq.8. More specifically, the QNTC problem assumes that each S-D pair perform QKD through one feasible path. By relaxing this assumption, the path of each f is permitted to be splittable. We formulate the following linear Program as LP_1.

$$\min \quad \alpha \sum_{p \in P} x_p + \beta \sum_{p \in P} y_p$$

$$S.t. \begin{cases} \sum_{t \in T_f} z_f^t = 1, & \forall f \in F \\ z_f^t \le x_p, & \forall p \in t, \forall t \in T_f, \forall f \in F \\ \sum_{f \in F} \sum_{p \in t : t \in T_f} z_f^t \cdot w_f \le y_p, & \forall p \in P \\ \sum_{f \in F} \sum_{e \in t : t \in T_f} z_f^t \cdot v_f \le c(e), & \forall e \in E \\ z_f^t \ge 0 \end{cases} \tag{2}$$

Note that the variables x_p, y_p, z_f^t are fractional in Eq.8 and we can solve it with a linear program solver in linear time. The optimal solution for this linear problem LP_1 is denoted by $\widetilde{x}_p, \widetilde{y}_p$ and $\widetilde{z}_f^t$. We use λ to present the result $\alpha \sum_{p \in P} x_p + \beta \sum_{p \in P} y_p$, so the optimal result is denoted by $\widetilde{\lambda}$. Since LP_1 is a relaxation of the QNTC problem, $\widetilde{\lambda}$ is a lower bound result of QNTC. Next, using the randomized rounding method, variable $\hat{z_f^t}$ is set to 1 with the probability of $\widetilde{z}_f^t$ while satisfying $\sum_{t \in T_f} z_f^t = 1, \forall f \in F$. It means that the S-D pair f selects path t if $\hat{z_f^t} = 1$.

D. Approximation Performance Analysis

We analyze the approximate performance of the proposed RQTC algorithm. Assume that the minimum capacity of all the data links is denoted by c_{min}. We define variable α as follows:

$$\alpha = min\{min\{\frac{c_{min}}{v_f}\}\}, min\{\frac{\widetilde{y}_p}{w_f}, p \in t, t \in T_f\}\} \tag{3}$$

Since RQTC is a randomized algorithm, we compute the expected relay numbers along with the traffic load on data links and quantum relays.

Quantum Relay Number. Considering that if any path t through p is selected, $\hat{x}_p$ is set to 1.We give the expected relay numbers as follows:

$$\mathbb{E}[\hat{x}_p] = 1 - \prod_{p \in t : t \in T_f} (1 - \widetilde{z}_f^t) \tag{4}$$

Theorem 2: The proposed RQTC algorithm achieves the approximation factor of L for quantum relay numbers, where L is the maximum number of feasible paths pass through any position $p \in P$.

Proof 3:

$$\begin{aligned} \mathbb{E}(\hat{x}_p) &= 1 - \prod_{p \in t : t \in T_f, f \in F} (1 - \widetilde{z}_f^t) \\ &\le \sum_{p \in t : t \in T_f, f \in F} \widetilde{z}_f^t \\ &\le L \cdot max_{p \in t : t \in T_f, f \in F}(\widetilde{z}_f^t) \end{aligned} \tag{5}$$

However, $\widetilde{x}_p = max_{p \in t : t \in T_f, f \in F}(\widetilde{z}_f^t)$, thus the approximation factor is L.

We first give two famous theorems for the following probability analysis.

Lemma 4: (Chernoff Bound):Given n independent variables:$x_1, x_2, ...x_n$, where $\forall x_i \in [0, 1]$.Let $\mu = \mathbb{E}[\sum_{i=1}^n x_i]$. Then $\mathbf{Pr}[\sum_{i=1}^n x_i \ge (1+\epsilon)\mu] \le e^{\frac{-\epsilon^2 \mu}{2+\epsilon}}$, where ϵ is an arbitrarily positive value.

Lemma 5: (Union Bound):Given a countable set of n events:$A_1, A_2, ..., A_n$, each event A_i happebs with possibility $\mathbf{Pr}(A_i)$.Then $\mathbf{Pr}(A_i \cup A_2 \cup ... \cup A_n) \le \sum_{i=1}^n \mathbf{Pr}(A_i)$

Quantum Device Number. We first give the approximate factor of the quantum channel number passing through of

each relay. The first step of the algorithm will derive a fractional solution for z_f^t ,x_p and y_p for the QNTC problem by linear program. Using th randomized rounding method, for each S-D pair $f \in F$, only one path in T_f will be chosen as its default route. Thus, the traffic load of relay p from S-D pair f is defined as a random variable $y_{p,f}$ as follows:

Definition 1: For each $p \in P$ and each $f \in F$, a random varialbe $y_{p,f}$ is defined as:

$$y_{p,f} = \begin{cases} w_f, with\ probability\ of\ \sum_{p \in t: t \in T_f} \widetilde{z}_f^t \\ 0, otherwise \end{cases} \tag{6}$$

According to the definition, the expected quantum traffic load in location p is:

$$\mathbb{E}[\sum_{f \in F} y_{p,f}] = \mathbb{E}[y_{p,f}] = \sum_{f \in F} \sum_{p \in t: t \in T_f} \widetilde{z}_f^t \cdot w_f \leq \widetilde{y}_p \tag{7}$$

Combining Eq.7 and definition of α, we have:

$$\begin{cases} \frac{y_{p,f} \cdot \alpha}{\widetilde{y}_p} \in [0,1] \\ \mathbb{E}[\sum_{f \in F} \frac{y_{p,f} \cdot \alpha}{\widetilde{y}_p} \leq \alpha] \end{cases} \tag{8}$$

Then, by applying Lemma 4, assume ϵ is an arbitrary positive value. It follows :

$$\mathbf{Pr}[\sum_{f \in F} \frac{y_{p,f} \cdot \alpha}{\widetilde{y}_p} \geq (1+\epsilon)\alpha] \leq e^{\frac{-\epsilon^2 \alpha}{2+\epsilon}} \tag{9}$$

Now we assume that:

$$\mathbf{Pr}[\sum_{f \in F} \frac{y_{p,f}}{\widetilde{y}_p} \geq (1+\epsilon)] \leq e^{\frac{-\epsilon^2 \alpha}{2+\epsilon}} \leq \frac{\Phi}{n} \tag{10}$$

where Φ is the function of network-related variables and $\Phi \to 0$ when the network size $n = |P|$ grows. The solution for Eq.10 is:

$$\epsilon \geq \frac{log\frac{n}{\Phi} + \sqrt{log^2\frac{n}{\Phi} + 8\alpha log\frac{n}{\Phi}}}{2\alpha}, n \geq 2 \tag{11}$$

We give the approximation performance as follows.

Theorem 6: The proposed RQTC algorithm achieves the approximation factor of $\frac{3logn}{\alpha} + 3$ for quantum device numbers.

Proof 7: Set $\Phi = \frac{1}{n^2}$,Eq.10 is transformed into:

$$\mathbf{Pr}[\sum_{f \in F} \frac{y_{p,f}}{\widetilde{y}_p} \geq (1+\epsilon)] \leq \frac{1}{n^3}, where\ \epsilon \geq \frac{3logn}{\alpha} + 2 \tag{12}$$

By applying Lemma 4, we have

$$\begin{aligned} &\mathbf{Pr}[\bigvee_{p \in P} \sum_{f \in F} \frac{y_{p,f}}{\widetilde{y}_p} \geq (1+\epsilon)] \\ &\leq \sum_{p \in P} \mathbf{Pr}[\sum_{f \in F} \frac{y_{p,f}}{\widetilde{y}_p} \geq (1+\epsilon)] \\ &\leq n \cdot \frac{1}{n^3} = \frac{1}{n^2}, \epsilon \geq \frac{3logn}{\alpha} + 2 \end{aligned} \tag{13}$$

Then the approximation factor of the algorithm is $\epsilon + 1 = \frac{3logn}{\alpha} + 2$

Data Link Capacity Constraints. Next, we analyze the performance of traffic load on data links. Similar to definition 1, we give another definition of random variable $\zeta_{e,f}$ as follows:

Definition 2: For each link $e \in E$ and each S-D pair $f \in F$, $\zeta_{e,f}$ is defined as:

$$\zeta_{e,f} = \begin{cases} v_f, with\ probability \sum_{e \in t: t \in T_f} \widetilde{z}_f^t \\ 0, otherwise \end{cases} \tag{14}$$

Similar to the proof before, we can proof that

$$\mathbf{Pr}[\sum_{f \in F} \frac{\zeta_{e,f} \cdot \alpha}{c(e)} \geq (1+\epsilon)\alpha] \leq e^{\frac{-\epsilon^2 \alpha}{2+\epsilon}} \tag{15}$$

Since there are at most n^2 links between $p \in P$, we can assume that:

$$\mathbf{Pr}[\sum_{f \in F} \frac{\zeta_{e,f}}{c(e)} \geq (1+\epsilon)] \leq e^{\frac{-\epsilon^2 \alpha}{2+\epsilon}} \leq \frac{\Phi}{n^2}, n \geq 2 \tag{16}$$

The solution is

$$\epsilon \geq \frac{log\frac{n^2}{\Phi} + \sqrt{log^2\frac{n^2}{\Phi} + 8\alpha log\frac{n^2}{\Phi}}}{2\alpha}, n \geq 2 \tag{17}$$

Similarly, by setting suitable values of parameters ϵ and Φ, we can derive the approximation performance on link capacity constraints.

Theorem 8: The proposed RQTC algorithm achieves the approximation factor of $\frac{4logn}{\alpha} + 3$ for data link capacity constraint.

Proof 9: Set $\Phi = \frac{1}{n^2}$,Eq.16 is transformed into:

$$\mathbf{Pr}[\sum_{f \in F} \frac{\zeta_{e,f}}{c(e)} \geq (1+\epsilon)] \leq \frac{1}{n^4}, where\ \epsilon \geq \frac{3logn}{\alpha} + 2 \tag{18}$$

By applying Lemma 4, we have

$$\begin{aligned} &\mathbf{Pr}[\bigvee_{p \in P} \sum_{f \in F} \frac{\zeta_{e,f}}{c(e)} \geq (1+\epsilon)] \\ &\leq \sum_{p \in P} \mathbf{Pr}[\sum_{f \in F} \frac{\zeta_{e,f}}{c(e)} \geq (1+\epsilon)] \\ &\leq n^2 \cdot \frac{1}{n^4} = \frac{1}{n^2}, \epsilon \geq \frac{4logn}{\alpha} + 2 \end{aligned} \tag{19}$$

Approximation Factor.

IV. Dynamic QKD Network Update

In this section, We first discuss scenarios where the path width requirements between endpoints change dynamically. Then we give solutions in these cases and propose approximation algorithms.

A. Dynamic Scenarios in QKD Network

In practice, the S-D pair set F may changes and the path width requirement w_f for each S-D pair f may changes too. When meeting these dynamic scenarios in QKD network, the number of quantum channels may exceed the capacity of a relay. At this time, we should re-select the path for every S-D pair, try to satisfy the quantum device constraint of each relay. However, considering devices are portable, when the quantum device constraints can not be satisfied anymore, we should update the quantum devices for each relay.

There are mainly three dynamic scenarios that will break constraints in QKD network. The first one is the change of S-D pair F. Considering that there are two quantum endpoints which were not communicating before want to perform quantum key distribution, we need to specify a path for them. The second is that the bandwidth required(either quantum bandwidth w_f or data bandwidth v_f) of one S-D pair f changes. Under such circumstances, the default path for f may need to be changed cause the quantum capacity of used relays may be not enough. The third dynamic scenario

is the failure of quantum devices. Once the device used fails, f may needs to select another path if the quantum bandwidth is not satisfied anymore. In more serious cases, a certain relay may fail completely or become untrustworthy due to some force majeure. At this time, we need to update the route as soon as possible, otherwise it will make QKD invalid for a long time, because the time to restore the relay can not be established.

B. QKD Routing Selection

In this section, we design an algorithm for QKD routing with data link capacity and quantum device capacity constraints after the QKD network topology is decided in section 3. Considering that we don't know how the secret bit rate requirement and data bandwidth will change and when the S-D pair f needs to communicate secretly, the proposed algorithm should be an online algorithm. We give the problem definition below. Note that the quantum relay set Q and variables y_p are decided in algorithm .III-C in section 3, and the candidate path set T_f for each S-D pair f is calculated on this new network topology.

As stated before, the S-D pair set F may change and the required bandwidth for both secret bit and data may change too. In some situation, the QKD network cannot serve everyone at the same time.We give a parameter $\lambda(f)$ to denote the benefit get if the QKD network serves S-D pair f. If we set $\lambda(f)$ to be w_f, then the S-D pair with higher secret bit rate has higher priority. Besides, if we set $\lambda(f)$ to be v_f, then the S-D pair with higher data bit rate has higher priority. We can also set $\lambda(f)$ to be $\frac{v_f}{w_f}$, that is , the secret level for f. Or we can simply see $\lambda(f)$ as benefits earned by providing QKD services. In general, the parameter λ_f is decided based on current QKD network environment by controllers or administrators. So our goal is to maximum the total benefit in the QKD network which is decided in section 3. The QKD routing problem is defined as follows:

$$\max \sum_{f\in F}\sum_{t\in T_f} z_f^t \cdot \lambda(f)$$
$$S.t. \begin{cases} \sum_{t\in T_f} z_f^t \le 1, & \forall f \in F \\ \sum_{f\in F, q\in t: t\in T_f} z_f^t \cdot w_f \le y_q, & \forall q \in Q \\ \sum_{f\in F}\sum_{e\in t: t\in T_f} z_f^t \cdot v_f \le c(e), & \forall e \in E \\ z_t^f \in \{0,1\} \end{cases} \quad (20)$$

The goal is to maximize the benefit of the quantum network, which is denoted as $\max \sum_{f\in F}\sum_{t\in T_f} z_f^t \cdot \lambda(f)$. The first set of inequalities means that the S-D pair f will choose a path. The second and third set of inequalities represent that the secret bit rate constraints and data link capacity constraints.

To solve the problem in Eq.20, we design an online algorithm based on the primal-dual, called PD-QRC. We give the dual problem of the linear relaxation of Eq.20.

$$\min \sum_{f\in F}\theta(f) + \sum_{q\in Q}\phi(q)\cdot y_q + \sum_{e\in E}\xi(e)c(e)$$
$$S.t. \begin{cases} \theta(f) \ge \lambda(f) - \sum_{q\in Q}\delta(f,t,q)\cdot w_f \cdot \phi(q) \\ \quad\quad - \sum_{e\in E}\delta(f,t,e)\cdot v_f \cdot \xi(e) & \forall f\in F, t\in T_f \\ \theta(f) \ge 0, & \forall f \in F \\ \phi(q) \ge 0, & \forall q \in Q \\ \xi(e) \ge 0, & \forall e \in E \end{cases} \quad (21)$$

The variables $\theta(f), \phi(q), \xi(e)$ are dual variables of the three sets of inequalities in Eq.(20) and these dual variables are non-negative. The function $\delta(f,t,q)$ and $delta(f,t,e)$ denote whether relay q and link e lie on the path t for S-D pair f.

$$\delta(f,t,q) = \begin{cases} 1, & \text{if S-D pair f routes through relay q in path t} \\ 0, & \text{otherwise} \end{cases}$$

$$\delta(f,t,e) = \begin{cases} 1, & \text{if S-D pair f routes through relay e in path t} \\ 0, & \text{otherwise} \end{cases}$$

Then we give the PD-QRC algorithm descirbed in Alg. **??**. The first step of our algorithm is to initialize dual variables defined before and three constants B,M and ϵ. B is defined as he maximum usage of each resource of all S-D pair f and all feasible path t.

$$B = max_{f,t}\{max_q \frac{\delta(f,t,q)\cdot w_f}{\lambda(f)}, max_e \frac{\delta(f,t,e)\cdot v_f}{\lambda(f)}\} \quad (22)$$

M is the number of inequalities from the second set to the fourth set in Eq.(20). In our algorithm, $M = |Q| + |E|$. The constant $\epsilon \in [0,1]$ represents the trade-off between the resource violation and network profit.

The second step is to choose a feasible path for each S-D pair f. When QKD network need to provide QKD services to f, we compute the profit of each path $t \in T_f$, which is denoted as K_t:

$$K_t = \lambda(f) - \sum_{q\in Q}\delta(f,t,q)\cdot w_f \cdot \phi(q) - \sum_{e\in E}\delta(f,t,e)\cdot v_f \cdot \xi(e) \quad (23)$$

Next we set $K \to max_{t\in T_f} K_t$, that is the maximum profit of all candidate paths for f. If $K<0$, providing QKD service to f does not bring any profit. If not, we choose efficient feasible path t^* for f. After that, we set dual variable $\phi(f)$ to be the maximum profit K and update dual variables $\phi(q)$ and $\xi(e)$ as the resources of quantum devices and links decrease.

The update of quantum device resources is as follows:

$$\phi(q) = \phi(q)[1 + \frac{\delta(f,t^*,q)\lambda(f)}{y_q}] + \epsilon\cdot\frac{\delta(f,t^*,q)\lambda(f)}{M\cdot y_q \cdot B}, \forall q \in Q \quad (24)$$

For data link resource, the update is as follows:

$$\xi(e) = \xi(e)[1 + \frac{\delta(f,t^*,e)\lambda(f)}{c(e)}] + \epsilon\cdot\frac{\delta(f,t^*,e)\lambda(f)}{M\cdot c(e)\cdot B}, \forall e \in E \quad (25)$$

C. Algorithm Performance Analysis

We analyze the approximate performance of the proposed PD-QRS algorithm in this section.

Definition 3: An online algorithm for QRS is said tobe $[\kappa, \psi]$ competitive if it achieves at least κ·OPT, where OPT

Algorithm 2 PD-QRS:Online Primal-Dual Algorithm for QKD Routing Selection

Step 1: Initialization
Initialize constants B,M and $\epsilon \in (0,1)$
Initialize variables $\theta(f), \phi(q), \xi(e) to 0, \forall f, \forall q, \forall e$
Step 2: Selecting Path for S-D pair f
for each feasible path $t \in T_f$ **do**
  Compute K_t by Eq. (23)
$K \rightarrow max_{t \in T_f} K_t$
if $K<0$ **then**
  Do not provide QKD services to f
else
  $t^* \rightarrow argmax_{t \in T_f} K_t$
  Perform QKD between S-D pair f by path t^*
  Update $\theta(f)$ as K
  Update $\phi(q)$ and $\xi(e)$ by Eqs. (24),(25)

is the optimal network profit for QRS, and constraints are violated by at most a multiplicative factor ψ.

The factor κ means how much profit we lose under the online scenario, and the factor ψ denotes how much of these resources exceed the capacity. Ideally, we want the algorithm to be [1,0] competitive, or at least $[\rho, 0]$ competitive for some $\rho>0$. However, the online algorithms with a positive competitive ratio can not avoid violating constraints.

Theorem 10: PD-QRS is $[(1-\epsilon), (logM + log(\frac{1}{\epsilon}))]$ competitive.

The theorem means that the online algorithm reaches a theoretical lower bound in terms of resource overloading and superior performance in terms of QKD network profit even if the secret and data routing rate is adversarial.

Under the dynamic scenario, the resource requirements for each $f \in F$ may change frequently. When the resource requirements of S-D pair f decrease, some occupied resources will be released and the dual variables will be decreased accordingly as in Eq. (26),(27)

$$\phi(q) = [\phi(q) - \epsilon \cdot \frac{\delta(f,t^*,q)\lambda(f)}{M \cdot y_q \cdot B}] / [1 + \frac{\delta(f,t^*,q)\lambda(f)}{y_q}], \forall q \in Q \tag{26}$$

$$\xi(e) = [\xi(e) - \epsilon \cdot \frac{\delta(f,t^*,e)\lambda(f)}{M \cdot c(e) \cdot B}] / [1 + \frac{\delta(f,t^*,e)\lambda(f)}{c(e)}], \forall e \in E \tag{27}$$

D. Discussion

However, there are chances that the quantum devices in some relays cannot satisfy all the requirements of S-D pair. In such situations, we do need to update the quantum devices in those relays. The update of quantum devices takes a relatively long time.During this period, we need to decide whether to provide QKD services for each f based on our online algorithm. Besides, we can incrementally update the quantum devices in each relay at a regular time to cope with the increased demand for quantum communications in the QKD network. For example, we can update the devices in each relay monthly, based on data in recent month, such as the maximum quantum channel bit rate. We give the generalized algorithm G-QRS described in Alg. IV-D

Algorithm 3 G-QRS:Generalized Algorithm for QKD Routing Selection

Step 1: Initialization
Initialize parameters as in PD-QRS
Initialize y_p based on current QKD network.
Step 2: Selecting Path for S-D pair f
Select paths for S-D pairs as in PD-QRS
Update $\phi(q), xi(e)$ with Eq.(26),(27)
Step 3: Updating quantum devices monthly
Update quantum devices in relay and y_q accordingly based on previous data.

V. Performance Evaluation

VI. Related Works

VII. Conclusion

References

[1] J. Y. Yen, "Finding the K Shortest Loopless Paths in a Network," *Management Science*, vol. 17, no. 11, pp. 712–716, July 1971.