Collaborative Routing in Partially-Trusted Relay based Quantum Key Distribution Optical Networks

Xingyu Zou[1], Xiaosong Yu[1], Yongli Zhao[1], Avishek Nag[2], and Jie Zhang[1]
[1]*State Key Laboratory of Information Photonics and Optical Communications (IPOC), Beijing University of Posts and Telecommunications, Beijing (BUPT), 100876, China*
[2]*School of Electrical and Electronic Engineering, University of College Dublin, Ireland*
**e-mail: {xiaosongyu, yonglizhao, lgr24} @bupt.edu.cn*

Abstract: This paper proposes a collaborative routing scheme in partially-trusted relay based quantum key distribution optical networks. Simulation results show it achieves good performance in terms of key distribution success rate.

1. Introduction

Quantum key distribution (QKD) technology provides theoretically unconditional point-to-point security based on fundamental quantum mechanics, and it has been used successfully in short-distance commercial applications. But for long-distance communication, relays in QKD are indispensable. There are three different relay-based QKD solutions: 1) Quantum relay based QKD. Quantum relay can realize the storage and forwarding of quantum states through quantum entanglement [1], thus realizing the long-distance distribution of quantum states. 2) Trusted relay based QKD. It caches the key generated by the point-to-point quantum key distribution link in trusted relay, and then transfer the end-to-end key by using the One-Time Pad (OTP) encryption algorithm hop-by-hop [2, 3]. 3) Measure-Device-Independent Quantum Key Distribution (MDI-QKD). In MDI-QKD, a pair of users transmits the signal to an untrusted relay located in the middle, which performs a Bell state measurement that projects the signals into a Bell state [4] and users can obtain secure key after post-processing, according to the measurement results which are announced in a public channel by the untrusted relay.

All the above three solutions have their disadvantages. Quantum relay based QKD is still under studied because of the immature of quantum memory; trusted relay based QKD is impractical since insecurity of certain relay sections cannot be ignored in the real world; and for MDI-QKD, there exists a limitation of the safety distance. In the near future, partially-trusted relay based QKD network seems to be more realistic, hence their corresponding constraints must be considered at the same time [5]. In addition, how to route in such a QKD optical networks is a significant but difficult issue [6]. This paper proposes a collaborative routing algorithm by considering both the trusted relays and untrusted relays to complete quantum key distribution in partially-trusted relay based QKD optical networks. Simulation results show that the proposed routing algorithm performs well in terms of key distribution success rate.

2. Relay based Quantum Key Distribution (QKD)

(1) ***Trusted relay based QKD.*** Fig. 1(a) illustrates the operations of trusted relay based QKD in details. Firstly, Alice sets up an initial secure key K1 with Node 2 by BB84 protocol. Similarly, Node 2 sets up a secure key K2 which is the same size of K1with Bob. Upon receiving service requests, Node 2 generates K'=K1⊕K2 by using a one-time pad algorithm (XOR) and sends it to Bob. Finally, Bob deciphers K' by K2⊕K' to obtain K1 and Bob shares the same secure key K1 with Alice.

(2) ***MDI-QKD.*** The fundamental of MDI-QKD is shown in Fig. 1(b). Firstly, both Alice and Bob send specially processed phase randomized weak coherent pulses to Node 2. Then, Node 2 works as a third-party detector to perform a Bell state measurement that projects the incoming signals into a Bell state for Alice and Bob. Finally, Alice and Bob share a secure key K1 after post-process. [4]

(3) ***Partially-trusted relay based QKD.*** Partially-trusted-relay QKD network offers co-existence of trusted relays and untrusted relays. As shown in Fig. 1(c), the flow charts of key generation, encryption, decryption, and relay between Alice and Bob in partially-trusted relay network are described. The main idea of this scheme is that the nodes can generate a secure key when there exists an untrusted relay by MDI-QKD and use it to encrypt the initial key by XOR, then send it to next node and the receiver node can decrypt it because the node shares the key with the sender node. Specifically, Node 2 encrypts K1 with K2 that are generated by Nodes 2 and 4 via MDI-QKD by XOR, (step2 to step3 in Fig. 1(c)). Then Node 2 sends the cipher text to Node 4 and Node 4 obtains K1 by deciphering it with K2 by XOR.

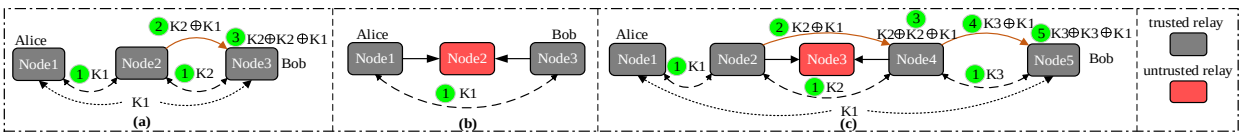

Fig. 1. (a) Trusted relay based QKD; (b) MDI-QKD; (c) Partially-trusted relay based QKD.

3. Collaborative Routing (CR) in partially-trusted relay based QKD

Collaborative Routing (CR) algorithm is designed by considering the working mechanism of trusted relays and untrusted relays, the security key is generated by the MDI-QKD when there exists an untrusted relay, and the key is generated by the BB84 protocol when there is no untrusted relay. So, trusted relays and untrusted relays can work collaboratively to distribute quantum keys. In order to describe CR algorithm clearly, this paper builds the following models. For simplicity, the network is designed as a 2-dimensional 4-connected grid mesh (4-C mesh) in Fig. 2(a). Each node is identified by its coordinates: $(i,j): i = 0,1 \ldots n\text{-}1; j = 0,1 \ldots n\text{-}1$. The distance of two nodes can be defined by $d[(i_1,j_1);(i_2,j_2)] = |i_2\text{-}i_1| + |j_2\text{-}j_1|$. Let N denote the number of network and T denotes the percent of trusted node in the network. Let $\mathrm{R}[S(i_S,j_S),D(i_D,j_D)]$ denote the request, where $S(i_S,j_S)$ denotes the source node and $D(i_D,j_D)$ denotes the destination node. This paper defines each node that performs routing as starting node and denotes it by P_S. Let θ_{P_S} represents the set of nodes with the distance of 1 or 2 from P_S, let $K(\theta_{P_S})$ represent the set of trusted nodes in θ_{P_S}, and let $S_{d_{MIN}}$ denote the node in $K(\theta_{P_S})$, which has not only the smallest d with $D(i_D,j_D)$ but also the key remaining. Let $\pi(S,D)$ denote the route table and F_R denote the flag whether the request is success or failed.

The pseudo-code for the CR algorithm is in Table.1. For each request, at first, the CR algorithm sets $S(i_S,j_S)$ as P_S and adds it to $\pi(S,D)$, then it finds the θ_{P_S} of P_S. After that, CR makes a judgement that whether the $D(i_D,j_D)$ is in θ_{P_S} or not. If it is in θ_{P_S}, it adds $D(i_D,j_D)$ to $\pi(S,D)$; if it is not in θ_{P_S}, CR will set a $S_{d_{MIN}}$ in $K(\theta_{P_S})$ as a new P_S and repeat the judgement until $D(i_D,j_D)$ is in θ_{P_S}. If $K(\theta_{P_S})$ is empty in a certain process, the request will be blocked and $\mathrm{F_R}$ will be marked as $FAILED$. Finally, if $\mathrm{F_R}$ is not $FAILED$, CR will traverse each node in $\pi(S,D)$ to judge whether there are optional relays with next node and choose the one with more key.

Figure 2 gives two examples of requests and corresponding key-distribution steps to show how CR works. Let us assume that the *request-1* is from *Node 5* to *Node 16*. Firstly, CR algorithm sets *Node 5* as P_S and find θ_{P_S}. Here assuming that the key is more probable to be in *Node 10* than in *Node 7*, CR chooses *Node 10* as $S_{d_{MIN}}$, and resets the $S_{d_{MIN}}$ as new P_S. Then, CR finds that the $S_{d_{MIN}}$ of *Node 10* is *Node 12*, so *Node 12* is set as new P_S. Finally, CR finds *Node 16* is in θ_{P_S} of *Node 12* and finishes the routing. CR and key distribution for *request-1* is shown in Fig. 2(b), where the numbers signify the order of key-distribution steps. As shown in Fig. 2(c), there are two situations of key distribution for *request-2* when distributing keys from *Node 3* to *Node 8*. For the first one, it is a completely trusted relay path; for the second one, it is a partially-trusted relay path. Which path to choose depends on the remaining keys of *Node 4* and *Node 7*, and CR will choose the one with more keys. In addition, it is necessary to note that the *step 1* in Figs. 2(b) and (c) is always ongoing even without a request.

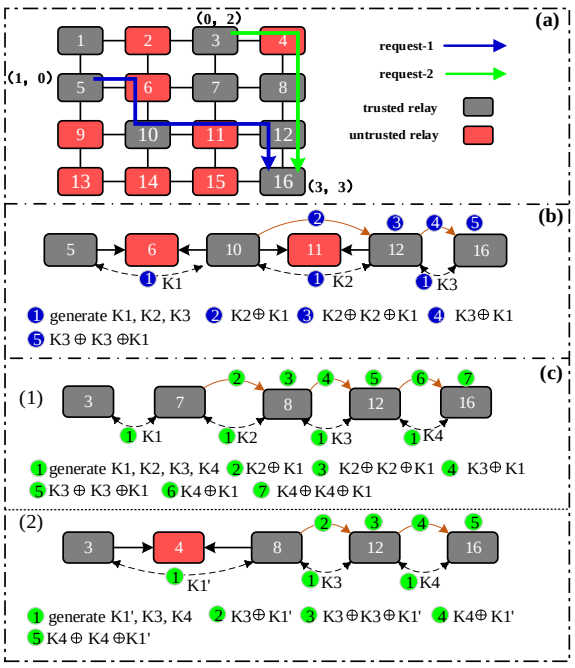

Fig. 2 (a) Network topologies; (b) Key distribution for *request-1*; (c) Key distribution for *request-2*.

Table 1. Collaborative routing algorithm

Collaborative Routing (CR) Algorithm

Input: network topology G(E, V), request $\mathrm{R}[S(i_S,j_S),D(i_D,j_D)]$
Output: $\pi(S,D)$, F_R

For each request $R[S(i_S,j_S),D(i_D,j_D)]$;
  Set $S(i_S,j_S)$ as the P_S and add it to $\pi(S,D)$;
  Find the θ_{P_S} of P_S;
  While $D(i_D,j_D) \notin \theta_{P_S}$, **do**
    If $K(\theta_{P_S}) \neq \emptyset$
      Add P_S to $\pi(S,D)$;
      Set $S_{d_{MIN}}$ as the new P_S;
      Find the θ_{P_S} of P_S;
    Else
      the request is blocked;
      Mark $F_R = FAILED$;
    End if
  End while
  If $\mathrm{F_R} \neq FAILED$
    Add $D(i_D,j_D)$ to $\pi(S,D)$;
    For each node in $\pi(S,D)$
      If ∃ *optional relays with next node*
        Choose one with more key;
        Add the relay to $\pi(S,D)$;
      End if
    End for
    Mark $F_R = SUCCEED$;
  End if
End for

4. Simulation results

To evaluate the performance of proposed Collaborative Routing (CR) algorithm, this paper simulates Key Distribution Success Rate (*KDSR*) in different kinds of network topologies. In the simulation, all the requests arrivals are assumed to obey Poisson distribution, and the trusted nodes and untrusted nodes are chosen following a uniform distribution. By considering different number of nodes in the network and different percent of trusted nodes, the simulation results that are obtained are shown in Fig. 3. Three kinds of network topologies are shown in Fig. 3(a). Figs. 3 (b), (c), and (d) are the simulation results for the ring network, the tree network, and the 4-C mesh network respectively. For simplicity, the simulation adopts a full binary tree with N nodes, for the tree network, and a N × N 4-C mesh network, so *N* is set as 7, 15, 31, 63, 127 in the tree network and 16, 36, 64, 100, 144 in the 4-C mesh network.

It can be observed that the *KDSR* gradually decreases for all three kinds of network topologies with the number of nodes increasing in Figs. (b), (c), and (d). This is because with *N* increasing and *T* fixed, the number of untrusted nodes is also increasing. Besides, the *KDSR* for all three network topologies tends to be stable and high as *T* is increasing which is intuitive. Figs. 3(e) and (f) show the performance comparison of CR in the three kinds of network topologies. The parameter settings are: *N*=100, *T*=10%, 30%, 50%, 70%, 90% in Fig. 3(e); *T*=50%, *N*=16, 36, 64, 100, and 144 in Fig. 3(f). It can be clearly observed that the *KDSR* in the 4-C mesh network is the best among the three network topologies in Figs. 3(e) and (f), and *KDSR* in the tree network is better than that in the ring network. This is because the 4-C mesh network has the highest connectivity whereas the ring network has the lowest. In general, the CR performs best in the 4-C mesh network among these three kinds of network topologies.

5. Conclusion

In the process of deploying QKD networks in the future, the partially-trusted relay will be a more realistic scenario. This paper is focuses on routing in such a scenario and proposes a CR algorithm in a partially-trusted-relay-based QKD optical network. Simulation results show that the proposed CR algorithm is effective for different kinds of QKD network topologies, especially for multi-connected networks.

Acknowledgement: this work is supported by NSFC project (61601052, 61971068, and 61822105), Fund of State Key Laboratory of Information Photonics and Optical Communications, BUPT (IPOC2019ZR01), and the Fundamental Research Funds for the Central Universities (2019XD-A05).

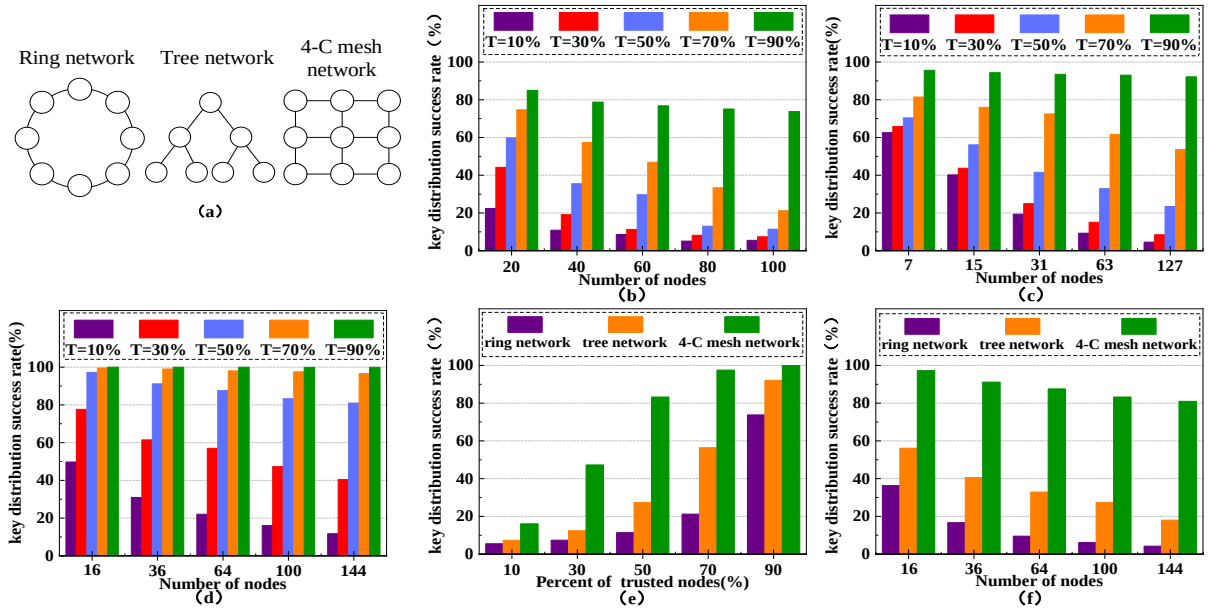

Fig. 3. (a) Three kinds of network topologies; (b) KDSR vs *N* in ring network; (c) KDSR vs *N* in tree network; (d) KDSR vs *N* in 4-C mesh network; (e) KDSR vs *T*; (f) KDSR vs *N*.

6. References

[1] D Collins et al. “Quantum relays for long distance quantum cryptography,” Journal of Modern Optics 52(5), 735-753 (2005).
[2] C Elliott. “Building the quantum network” [J]. New Journal of Physics, 4(1), 46 (2002).
[3] M Sasaki, et al. “Field test of quantum key distribution in the Tokyo QKD Network,” Optics express 19(11), 10387-10409 (2011).
[4] HK Lo et al. “Measurement-device-independent quantum key distribution,” Physical review letters 108.13, 130503 (2012).
[5] E Diamanti et al. “Practical challenges in quantum key distribution,” npj Quantum Information 2, 16025 (2016).
[6] YL Zhao et al. “Resource allocation in optical networks secured by quantum key distribution,” IEEE Communications Magazine 56.8, 130-137 (2018).