Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **1**, January **2014**

A Novel QKD Network Routing Algorithm Based on Optical-Path-Switching

Qi Han, Liyang Yu, Wenchao Zheng, Na Cheng, and Xiamu Niu

School of Computer Science and Technology
Harbin Institute of Technology
Harbin, 150001, China
qi.han@hit.edu.cn

Received March, 2013; revised May, 2013

Abstract. *The hybrid model of QKD(Quantum Key Distribution) network is a reasonable approach to build a quantum cryptographic network in the current phase which combines the optical switcher and the trusted repeater to attain the security and the scope of the network. The core network of this model is connected and routed by optical switchers, and is extended in spacial scale by the trusted repeater. This paper focuses on the routing method in the core network. Since the quantum path established by the optical switchers is monopolized by the current pair of Alice and Bob, the routing algorithm of the conventional network couldn't deal with such a dynamic graph. More factors would be considered to find and keep an optical path in a dynamic graph. Based on a cost function of the optical path define in this paper, an multi-path search algorithm is proposed to find available optical paths and select a best path as the route of one process of key distribution. Experiments raised on NS2 demonstrates the validity and effectiveness of the proposed algorithm.*
Keywords: QKD network, optical switcher, routing algorithm

1. **Introduction.** Since the principle of Quantum Key Distribution(QKD) was brought up and demonstrated in laboratory, lot of efforts was devoted into the realization of QKD system and further, the QKD network[1]. The point to point QKD system was investigated since 1990s, and the effective distance of key distribution had achieved more than $100km$. More complex system was tested which involved more elements such as switcher, multi-users, storage and transmitting of keys, etc[1, 2, 3, 4]. A QKD network compatible with the current network was promoted by the necessary of secure applications and systems. The most significant different between QKD network and the conventional network is that the key distribution pair in QKD network will monopolize the path they use it as a quantum channel while the communication pairs in conventional network always share paths in the graph of network. This is the motivation of the research works devoted into the construction and routing of a QKD network.

Till now the techniques to build QKD network can be divided into three categories, which is based on the trusted repeater, the optical-path-switching and the combination of them. In 2004, Austria set up SECOQC project and four years later the QKD experiment network based on the trusted repeater was successfully established in Vienna[5, 6, 7]. This kind of QKD network is easy to implement and extend. The U.S. IARPA reported the first QKD experiment based on optical-path-switching[8], which was able to support multiple users at the same time without guaranteeing the credibility of the intermediate nodes.

However, it couldn't support long-distance communication[9]. In 2009, Pan's team in USTC developed a hybrid network based on the optical-path-switching device designed by themselves and the trusted repeater, this network achieved the interconnection between any two nodes and extend the communication distance[10].

The hybrid QKD network can not only overcome the QKD distance limitations, but also reduce the number of trusted repeater nodes. Therefore this kind of QKD network is more flexible, scalable and reliable. And there also more issues need to be considered to design and construct a large scale hybrid QKD network, such as the framework of the system, the routing algorithm in the hybrid network, the protocol to join the quantum channel and the traditional communication channel, etc[11, 12, 13]. This paper proposed our works on the design of the hybrid QKD network model and the design of routing algorithm in a dynamic-path network. The QKD network is divided into different domains, each domain is a local network routed by optical switchers, and the domains are connected by the trusted repeaters. In another point of view, the QKD network can be considered as two layer: the quantum path layer and classical network layer. The classical network layer support the establish of the quantum path besides the function of the communication in the classical manner. The existing QKD routing technology is not competent in managing the QKD network, for it can only support few nodes of each domain. So we investigated and designed the routing algorithm for the network of each domain to support larger domains, and the QKD network could run automatically by the support of the new designed routing protocol.

This paper is organized as follows. In section 2, the model of the QKD network is discussed and improved, the concept of "Pilot Signal" is proposed. In section 3, a quantum link model is established and a new routing algorithm is proposed. The demonstrating experiments and the results is shown in section 4, and the feasibility of the proposed algorithm is proved. Finally, the conclusions are given in Section 5.

2. The Model of QKD Network.

According to the basic principles of basic quantum mechanics, such as Heisenberg uncertainty principle and quantum no-cloning theorem, the state of the quantum as the information carrier in the quantum network can't be measured or cloned[14, 15]. And the storage and replication of quantum states still can't be achieved under the existing technical conditions. Therefore it's impossible for the classic network routing mechanisms to be applied in the quantum network[16, 17]. Depending on the QKD communication characteristics, post-processing of quantum key distribution needs the support of the classic channel for quantum router. So it is the routing device built on the classic router that accomplishes the storage and routing for classic data packets. From this view, we designed the QKD network model as shown in Figure 1. In this model, if there is a quantum link between any two quantum routers, a classic link should be established, but not vice versa. When any two nodes want to communicate with each other through the quantum channel, the starter needs to send a signal through the classic channel to find an available path in the quantum channel. The calling information is define as "pilot signal" in our work.

In order to support the pilot signal for searching path, an appropriate routing algorithm is necessary. During the quantum communications, the attenuation of the signal causes communication BER (Bit Error Rate) increased. What's more, when the photons pass the optical switch it will lead to additional attenuation of the signal. Therefore, both the cost of the quantum link and the cost of optical switch should be taken into consideration.

3. **The Proposed Routing Algorithm.** In this section, we first introduce the model to describe the cost of quantum path, and based on this model we present the definition of the cost of quantum path. Then, a routing algorithm fits for the dynamic quantum network is proposed.

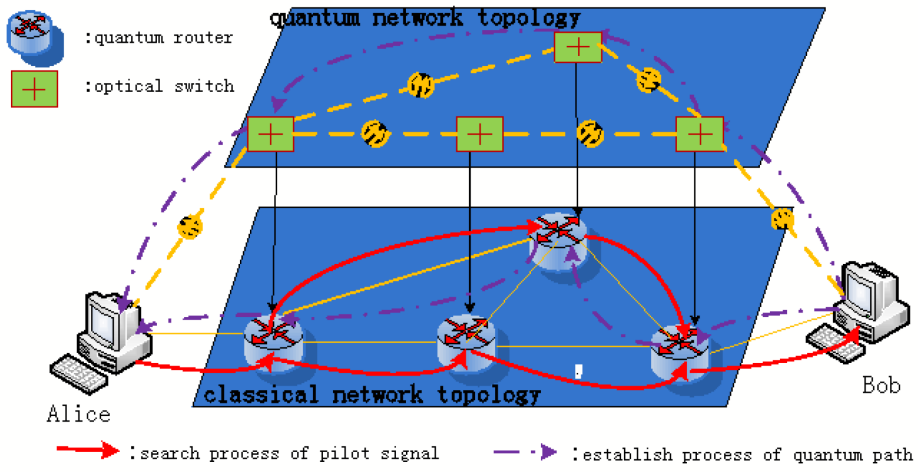

FIGURE 1. The tow layer model of QKD network

3.1. **Quantum Link Model.** As mentioned above, a quantum link model is necessary to describe the cost of quantum path which is an important parameter for the routing algorithm. As shown in figure 2, the simple weighted graph $G = (V, E)$ represents a QKD network, where V, E denote the nodes set and the edges set, respectively. v is any one of the elements in V, representing a quantum network router while e is an arbitrary element in E representing a quantum communication link in the network. Due to the transmission loss of the quantum state information, each e has a quantum link cost metric $L(e)$. For any one node, since the insertion loss of the introduction of the optical switch, it has a node cost metric $2 * N(v)$. As shown in Figure 2, for each path like $v1- > v2- > v3$, the cost of quantum path from node $v1$ to node $v3$ is $C(v1, v3) = N(v1) + L(< v1, v2 >) + 2 * N(v2) + L(< v2, v3 >) + N(v3)$. Its obvious that for a link $< v1, v2 >$ with a quantum link cost $L(< v1, v2 >)$, there are two nodes $v1$ and $v2$ corresponding to the cost of the optical switch. So we can incorporate the corresponding node cost into the quantum link cost, then we get the new quantum link cost $C(v1, v2) = N(v1) + L(< v1, v2 >) + N(v2)$. The other quantum link costs can be calculated in the same way. Thus, we can find that, $C(v1, v3) = C(V1, V2) + C(v2, v3)$. Through the transformation process, the node cost is introduced into the quantum link cost. Meantime, we also introduce $f(< v, w >)$ to measure the cost of the hops' number and this function f represents the network connectivity's influence. In order to get the best path with the constraints of the quantum link cost and the number of hops, we can convert the best-path-choosing problem into multi-plus-path-choosing problem by weighting processing or logarithmic processing methods and so on.

3.2. **The Cost of Quantum Path.** According to the model above, we de
ne the cost of quantum path as follows:

$$\cos t < s, d >= \alpha \times \sum C(< x, y >) + \beta \times f(< s, d >)$$

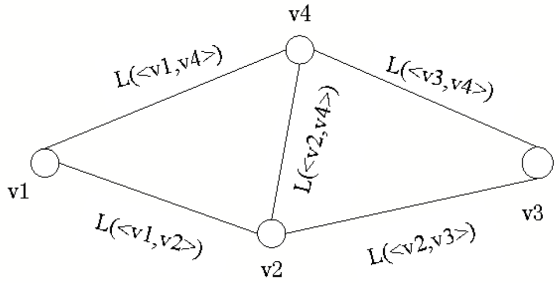

FIGURE 2. Quantum Link Model

where $x, y \in V, < x, y > \in E$, s is the communication source terminal, d is the destination end, $\alpha + \beta = 1$. The process of path selection can be influenced with this cost value by adjusting α and β, changing link cost and the number of the hops.

3.3. **The Routing Algorithm.** Because of the exclusivity of the link and the light switch during the communication between any two nodes, it's not feasible to provide only the best path for the pilot signal routing when the link or the optical switch is temporarily occupied. However, there may be a suboptimal feasible path to choose for the entire network in fact, so we should provide multiple independent feasible paths for the pilot signal and give it more chances to get the better available path. We call the algorithm MPSA(Multi-Path Search Algorithm), which is based on the Dijkstra algorithm.

The proposed MPSA algorithm's basic idea is as follows. The shortest path from one node to any other one in the network can be obtained with the edge weight by using Dijkstra algorithm. In the same way, after updating the edge weights in the network topology with the iterative factor method, the corresponding sub-optimal path will be obtained. And all possible sub-optimal paths will be found out in the cost-increasing order. Then we can get the routing table from one node to any other node. Finally the order of the hop nodes in the routing table needs to be adjusted through referring to those next-hops' idle status.

In order to increase the success rate for the pilot signal establishing a QKD path, the proposed algorithm takes full account of the three different impact factors in the QKD path selection process, i.e., the idle status of the next-next hop node, the number of the hops and the link cost. The algorithm to find the available feasible paths from a source node to any other one is detailed as follows.

Step 1: Input the quantum network topology G = (V, E)and the set of the destination node $D = \{d | d \in V\}$.

Step 2: Calculate the shortest path from node s to any other node in the network topology G by using Dijkstra algorithm and record them. Calculate the quantum link costs of theses paths and then make sure whether the destination can be reached. If the link cost is greater than MAXLENGTH, i.e., the longest distance of QKD, the destination node is unreachable and should be removed from D.

Step 3: If D is empty, go to Step 6, else calculate the sub-optimal path from node s to node $d \in D$. Increase the link cost of the shortest path from node s to node d by k times. And mark the state of the next-hop from node s to node d as unreachable. Then we get a new network topology $\acute{G}$ whose edge weight values are iteratively changed.

Step 4: Calculate the shortest path from node s to any other node in the network topology Ǵ by Dijkstra. If the shortest path is found, record this path and its link cost. Make sure whether the node d is reachable by these link costs. If it's reachable, make it the sub-optimal path from node s node d else remove d from D, and then go to Step3.

Step 5: Increase the link cost of the sub-optimal path from node s to node d by k times. Mark the state of the next-hop as unreachable. Update the network topology Ǵ and go to Step4.

Step 6: Get the routing table whose next-hops have been sorted by the link cost of the path. Adjust the next-hop's priority by referring the idle degree of the corresponding optical switch. The idle degree has four types which are shown as follows:

- Type 0: Next-hop p is occupied, and can't be used. Take the path as an alternate path. When the port goes available, go to Step 6.
- Type 1: Next-hop p is available, idle degree $L(p) = 1$ indicating p gets a relatively greater idle degree and so that it is suitable as the next-hop for routing. Take this kind of path as the optimal candidate path. Sort these paths according to their costs.
- Type 2: Next-hop p is available, idle degree $L(p) = 0.5$ indicating the ports of p are available, but if it was used as the next-hop, it might be occupied and unable to reach their destinations. Take this kind of path as the sub-optimal candidate path. Sort these paths according to their costs.
- Type 3: Next-hop p is busy, idle degree $L(p) = 0.5$ indicating that only few ports of p are available. If it was used as the next-hop, it would be very likely occupied and unable to reach their destinations. Take this kind of path as the sub-optimal candidate path. Sort these paths according to their costs.

4. **Experiments and Results.** The testing of the proposed algorithm based on the simulation of the QKD network. Figure 3 is the testing QKD network topology simulated based on NS2. The nodes 0 to 9 are quantum routers and the nodes 10 to 14 are five end users. Suppose that the quantum link and the classic link are completely corresponding to each other. Since the QKD is essentially a kind of end-to-end communication and the

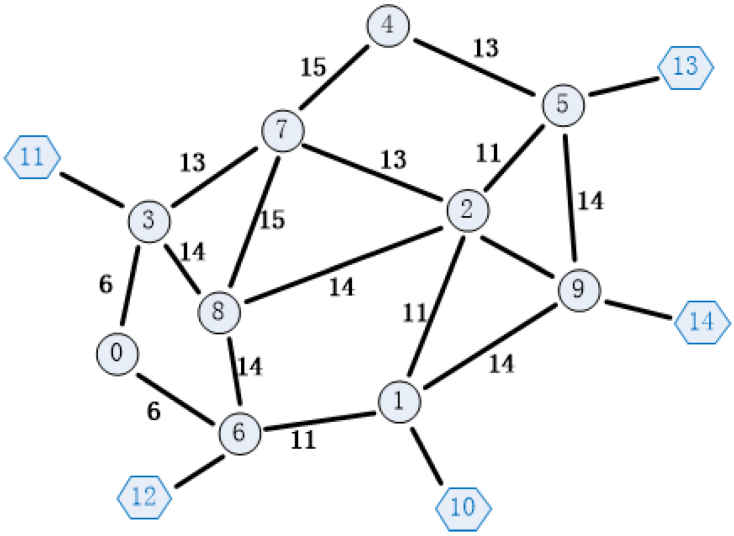

FIGURE 3. The topology of the test network

pilot signal routing is just considering the optional routing to reach the end-user nodes, we can only calculate those paths from the quantum routers to the end-users. The test results are shown in figure 4 and figure 5.

From the routing table of node 2 and node 6, we can see that the tables include multiple paths to each destination that can be reached. Observing the paths from node 2 to destination 13, although the cost of the path [7 4 5 13] is less than path [1 9 5 13], for the path [1 9 5 13] crosses with the optimal path [5 13], it gives more preference to path [7 4 5 13] for its relatively higher independence. The experimental results show that the algorithm takes into consideration not only the cost of the quantum link and the optical switch, but also the independence of each path.

```
######################################################################
myId:2
dest:10
       (nextHop:1 , cost:41, route:[1 10])
       (nextHop:9 , cost:74, route:[9 1 10])
       (nextHop:8 , cost:99, route:[8 6 1 10])
       (nextHop:7 , cost:139, route:[7 3 0 6 1 10])
       (nextHop:5 , cost:99, route:[5 9 1 10])
dest:11

       (nextHop:7 , cost:71, route:[7 3 11])
       (nextHop:8 , cost:73, route:[8 3 11])
       (nextHop:1 , cost:109, route:[1 6 0 3 11])
       (nextHop:5 , cost:127, route:[5 4 7 3 11])
       (nextHop:9 , cost:187, route:[9 1 6 8 7 3 11])
dest:12
       (nextHop:1 , cost:67, route:[1 6 12])
       (nextHop:8 , cost:73, route:[8 6 12])
       (nextHop:7 , cost:113, route:[7 3 0 6 12])
       (nextHop:9 , cost:100, route:[9 1 6 12])
       (nextHop:5 , cost:158, route:[5 4 7 8 6 12])
dest:13
       (nextHop:5 , cost:41, route:[5 13])
       (nextHop:9 , cost:74, route:[9 5 13])
       (nextHop:7 , cost:101, route:[7 4 5 13])
       (nextHop:1 , cost:99, route:[1 9 5 13])
       (nextHop:8 , cost:132, route:[8 7 4 5 13])
dest:14
       (nextHop:9 , cost:45, route:[9 14])
       (nextHop:1 , cost:70, route:[1 9 14])
       (nextHop:5 , cost:70, route:[5 9 14])
       (nextHop:8 , cost:128, route:[8 6 1 9 14])
       (nextHop:7 , cost:130, route:[7 4 5 9 14])
######################################################################
```

FIGURE 4. Routing Table of Nodes 2

```
######################################################################
myId:6
dest:10
       (nextHop:1 , cost:41, route:[1 10])
       (nextHop:8 , cost:99, route:[8 2 1 10])
       (nextHop:0 , cost:172, route:[0 3 7 2 9 1 10])
dest:11
       (nextHop:0 , cost:57, route:[0 3 11])
       (nextHop:8 , cost:73, route:[8 3 11])
       (nextHop:1 , cost:123, route:[1 2 7 3 11])
dest:12
       (nextHop:12 , cost:15, route:[ 12])
dest:13
       (nextHop:1 , cost:93, route:[1 2 5 13])
       (nextHop:8 , cost:99, route:[8 2 5 13])
       (nextHop:0 , cost:143, route:[0 3 7 4 5 13])
dest:14
       (nextHop:1 , cost:70, route:[1 9 14])
       (nextHop:8 , cost:103, route:[8 2 9 14])
######################################################################
```

FIGURE 5. Routing Table of Nodes 6

5. **Conclusions.** The properties of the QKD communication make the classic network routing technologies cannot be applied to the quantum network. Through establishing a new quantum link model and defining the cost of the quantum path, we propose a novel network routing algorithm for the QKD based on optical-path-switching. And the experiments and results demonstrate its validity and effectiveness.

Acknowledgement. This work is supported by the National Natural Science Foundation of China (61100187), the Fundamental Research Funds for the Central Universities (Grant No. HIT. NSRIF. 2010046) and the China Postdoctoral Science Foundation(2011M500666).

REFERENCES

[1] E. Biham, B. Huttner, and T. Mor, Quantum cryptographic network based on quantum memories, *Journal of Physical Review A*, vol. 54, no. 4, pp. 2651-2658, 1996.

[2] P. D. Townsend, Quantum cryptography on optical fiber networks, *Journal of Optical Fiber Technology*, vol. 4. no. 4, pp. 345-370, 1998.

[3] P. Xue, C. F. Li, and G. C. Guo, Conditional efficient multiuser quantum cryptography network, *Journal of Physical Review A*, vol. 65, no. 2, pp. 022317.1-022317-7, 2002.

[4] P. D. Townsend, Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing, *Journal of Electronics Letters*, vol. 33, no. 3, pp. 188-190, 1997.

[5] A. Poppe, M. Peev, and O. Maurhart, Outline of the SECOQC quantum-key-distribution network in vienna, *International Journal of Quantum Information*, vol. 6, no. 2, pp. 209-218, 2008.

[6] T. Länger, and G. Lenhart, Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD, *New Journal of Physics*, vol. 11, no. 5, pp. 055051-1-055051-16, 2009.

[7] M. Peev, C. Pacher, and R. Alleaume, et al., The SECOQC quantum key distribution network in Vienna, *New Journal of Physics*, vol. 11, no. 7, pp. 075001-1-075001-4, 2009.

[8] T. E. Chapuran, P. Toliver, and N. A. Peters, et. al., Optical networking for quantum key distribution and quantum communications, *New Journal of Physics*, vol. 11, no. 10, pp. 105001-1-105001-17, 2009.

[9] A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, Y. Nambu, and A. Tomita, Recent progress in quantum key distribution network technologies, *Proc. of European Conference on Optical Communications*, pp. 24-28, 2006.

[10] T. Y. Chen, J. Wang, and H. Liang, et. al., Metropolitan all-pass and inter-city quantum communication network, *Journal of Optics Express*, vol. 18, no. 26, pp. 27217-27225, 2010.

[11] M. Fu, F. Zhao, Y. Lu, and S. Liu, Progress of practical quantum key distribution network, *Journal of Laser & Optoelectronics Progress*, no. 10, pp. 39-47, 2007.

[12] Y. Liu, H. M. Qu, W. Y. Liu, C. Q. Wang, and J. T. Yang, Scheme design and improvement of quantum key distribution network, *Chinese Journal of Quantum Electronics*, vol. 22, no. 5, pp. 699-703, 2005.

[13] G. Chen, Z. B. Wu, and B. J. Yang, Architecture and performance analysis of quantum key distribution network, *Journal of Optical Communication Technology*, vol. 32, no. 11, pp. 58-61, 2008.

[14] Z. S. Yuan, Y. A. Chen, Z. Bo, and S. Chen, Experimental demonstration of a BDCZ quantum repeater node, *Journal of Nature*, vol. 454, no. 7208, pp. 1098-1101, 2008.

[15] Z. B. Chen, B. Zhao, Y. A. Chen, J. Schmiedmayer, and J. W. Pan, Fault-tolerant quantum repeater with atomic ensembles and linear optics, *Journal of Physical Review A,*, vol. 76, no. 2, pp. 022329-1-022329-12, 2007.

[16] C. Clausen, I. Usmani, and F. Bussieres, et. al., Quantum storage of photonic entanglement in a crystal, *Journal of Nature*, vol. 469, no. 7331, pp. 508-511, 2011.

[17] J. J. Longdell, E. Fraval, M. J. Sellars, and N. B. Manson, Stopped light with storage times greater than one second using electromagnetically induced transparency in a solid, *Journal of Physical Review Letters*, vol. 95, no. 6, pp. 063601-1-063601-4, 2005.