A Quantum Cryptography Communication Network Based on Software Defined Network

Hongliang Zhang [1,*], *Dongxiao* Quan [1,*], *Changhua* Zhu[1,*], and *Zhigang* Li[1,*]

[1]Skate Key Laboratory of Integrated Services Networks, XiDian University, Xi'an, Shaanxi, China

Abstract. With the development of the Internet, information security has attracted great attention in today's society, and quantum cryptography communication network based on quantum key distribution (QKD) is a very important part of this field, since the quantum key distribution combined with one-time-pad encryption scheme can guarantee the unconditional security of the information. The secret key generated by quantum key distribution protocols is a very valuable resource, so making full use of key resources is particularly important. Software definition network (SDN) is a new type of network architecture, and it separates the control plane and the data plane of network devices through OpenFlow technology, thus it realizes the flexible control of the network resources. In this paper, a quantum cryptography communication network model based on SDN is proposed to realize the flexible control of quantum key resources in the whole cryptography communication network. Moreover, we propose a routing algorithm which takes into account both the hops and the end-to-end availible keys, so that the secret key generated by QKD can be used effectively. We also simulate this quantum cryptography communication network, and the result shows that based on SDN and the proposed routing algorithm the performance of this network is improved since the effective use of the quantum key resources.

1 Introduction

The one-time-pad encryption scheme can guarantee unconditional security of information transmission in the traditional communication network. But one-time-pad is unrealistic until QKD is raised. The unconditional security of QKD is guaranteed by the basic principles of quantum mechanics, that is, Heisenberg's uncertainty principle and quantum non-cloning theorem. The quantum cryptography communication network which is based on QKD and one-time-pad can achieve the secure transmission of information. The architecture of the quantum cryptography communication network generally includes three layers: application layer, key management layer, and quantum layer.

The quantum layer is used to implement the end-to-end QKD and upload the generated key to the key management layer. The key management layer is used to store the keys generated by the quantum layer and select the appropriate route. Application layer is used for the access of diverse transaction, including voice, video and other transaction. The

*Corresponding author: luffyliang@163.com

information is encrypted with the key stored by the key management layer for secure transmission. Compared with the classical network, the session key is transmitted by a sequence of links that protected by QKD protocols in quantum cryptography communication network. Apparently, the establishment of communication is limited by link keys[1]. So it is important to be able to control link keys throughout the network.

In the traditional network, most of proposed algorithms can usually realize the local optimal solution, because the topology of the whole network is unknown. Besides, if we continue to use the classical routing algorithms in quantum communication network, such as RIP algorithm. Since this alogrithm is based on hops, it means the routes that have the minimal number of hops will be chosen repeatedly as optimal routes, which implies the network will eventually fail to communicate, due to the keys in those links will be depleted in a short time. Meanwhile, the keys in the links that are rarely used will be severely wasted, since those links are never considered as the optimal routes.

SDN is an emerging and fast growing technology for interconnecting network devices and forwarding packets based on unified policies and security enforcements[2][3]. SDN offers deep programmability of the network at all layers and even extends the network state into applications for enabling better pathing decisions. The OpenFlow protocol plays a key role in enabling SDN architectures through its simple, flexible and adaptable programming interface[4] At present, the mainstream SDN architecture is mostly devised according to the three-tier model, that is, the application layer, the control layer, and the forwarding layer , which are illustrated in Fig. 1.

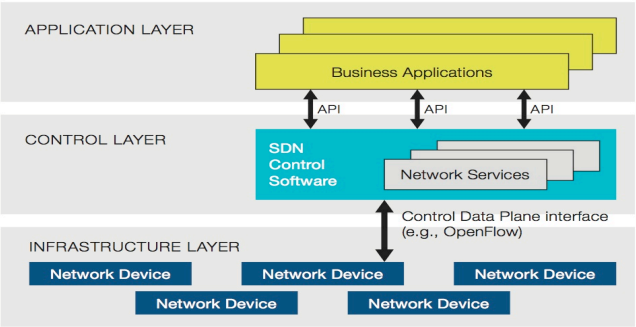

Fig. 1. Mainstream SDN architecture

In this paper, first, we propose a quantum cryptography communication network model based on the traditional SDN architecture, which makes full use of the characteristics of SDN and can realize the visualization of link keys in the whole network and select the global optimal route of point-to-point according to the key statistics result. Second, we propose an adaptive routing algorithm, which can automatically select the optimal route.

The rest of this paper is organized as follows. In section 2, we will describe in details the composition and operation principle of the quantum cryptography communication network we designed. In section 3, a simulation platform is set up and is used to count the amount of the available keys in the whole network links. Then in section 4, we propose a quantum communication network routing algorithm and make a simulation on it. In the last section, we make our main conclusion and discuss some remaining questions in this paper.

2 Design of network architecture model

We design the quantum cryptography communication network based on trusted repeaters[5]. The nodes in the network are divided into relay nodes and terminal node. The terminal node

has three layers: the application layer, the network layer and the quantum layer. The main function of the application layer is to access voice, video, ftp and so on. The role of the network layer is to establish a network connection and provide services for the upper. Quantum layer implements end-to-end QKD. In the division of the protocol layer, the terminal node of both our network and the traditional network are consistent in function. The reply node is divided into quantum layer[6]and middle layer[4][7].

We will explain our network reply model architecture in details with end-to-end communications as shown in Fig.2.

The quantum layer we design refers to the QKD module[8], and it utilizes QKD protocols to generate keys. Considering all implementations of practical QKD systems are based on optical apparatus, so we suppose the quantum layer consists of single photon sources, modulators, detectors and other optical components[9]. It would be very ideal if the QKD module can communicate directly with the controller, but it is not yet possible[10]. So we design the middle layer. The middle layer has two parts: the key storage layer and the OpenFlowAgent (OFA) layer. The key storage layer is used to store the keys generated by the quantum layer, and report the number of keys to OFA in time. The OFA is an extended OpenFlow switch that acts as a proxy for QKD modules to communicate with the key management layer. We choose the SDN controller as the key management layer because it can monitor the whole network topology information in real time and control the network resources such as bandwidth in the traditional network, and effectively improve the utilization of network resources. Since key resources are relatively valuable in quantum cryptography communications, so we take advantage of of SDN controllers to effectively manage key resources. The key management layer has two roles, one is to act as a traditional SDN controller, and the other is to control the entire network key state. This means it will send two kinds of flowtables to the OpenFlowAgent, one of them is responsible for the direction of traditional network data, and the other is responsible for the direction of data encrypted by the quantum key. The reason we designed the two flow tables is the encrypted data can not be transmitted due to the key amount is insufficient, but the transmission of the conventional data can not be affected by this reason. When a data message passes through the SDN relay node, it will selectively match the flowtable[2].

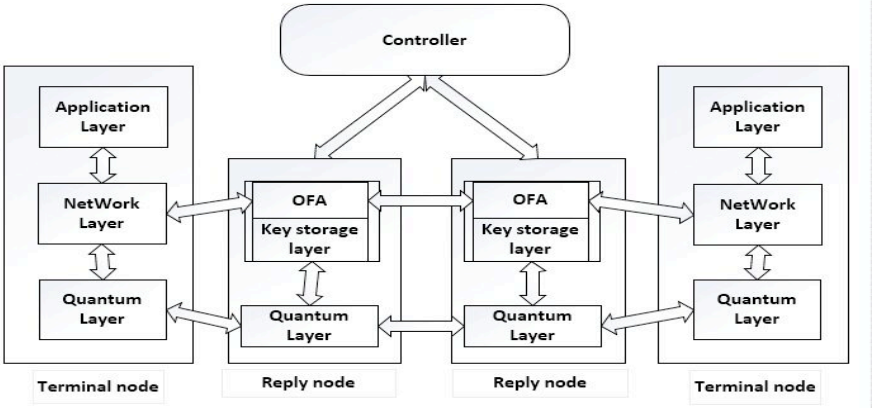

Fig. 2. Hierarchical model architecture

The communication process of each layer is shown in Fig.3 The OFA layer is in charge of encapsulating the key information, which is stored in the key store layer, into the PacketIn packet and uploading the packet to the key management layer[10]. At this point, the key management layer knows the keys state in the entire network. The key management layer selects the globally optimal route according to the key state of the whole network,

then it sends the routing information to the OFA through the flow table. Finally, the application layer communicates with each other through the route[4].

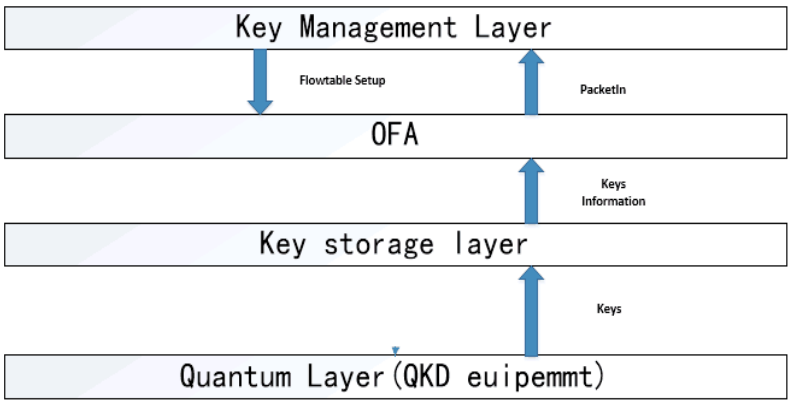

Fig. 3. Communication process

We make a network simulation according to the model and ideas mentioned in Sec.2 to verify the performance of the SDN controller manages the network key state.

We use Mininet to generate the network topology. Mininet is a powerful network simulator that is especially useful for experimenting with SDN applications[4]. To simply explain, one can pass it a file specifying the topology that one want to simulate and it establishes the environment using the Linux namespace software. The controller used in our simulation model is the mainstream SDN controller Floodlight since its stability and ease of use have been praised by SDN professionals. With these two softwares, we build our experimental simulation platform on the Linux system.

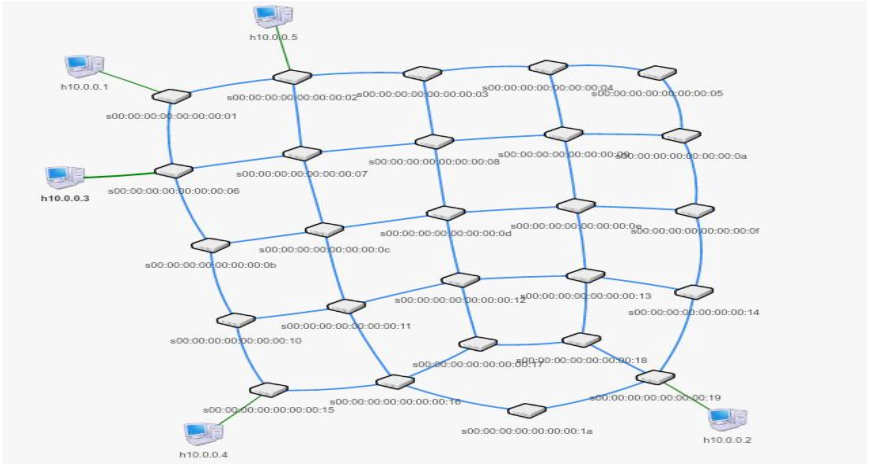

Fig. 4. Network topology

Now we assume that the quantum layer has already generated keys and upload the key to the key store layer. The key management layer needs to poll the nodes in a certain cycle to obtain the global network key state. The network topology generated by Mininet is shown in Fig.5. Here, Each switch node in the topology can be connected to a number of host nodes. We configure five hosts (h10.0.0.1 , h10.0.0.2 , h10.0.0.3 , h10.0.0.4 and h10.0.0.5) in this topology.

3 Quantum key management simulation

We will find the link through the following steps and learn the information of key in this link:
1. The link discovery module of the key management layer initiates a thread to monitor on the entire network topology, and the thread runs according to a certain time interval.
2. The key management layer uses the Link Discovery Protocol (LLDP) to learn the link state.
3. The link discovery module updates in time the key state of each link stored in the key management layer and timely displays in the console.

The following is a small part of the display as shown in Fig.5.

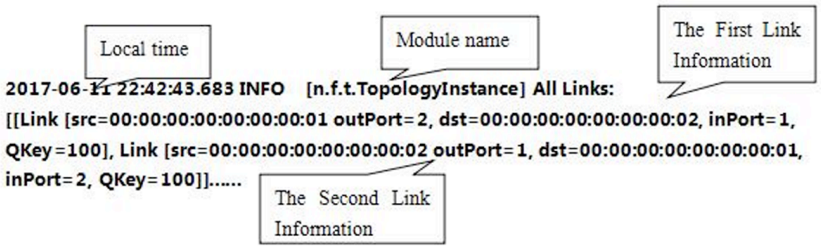

Fig. 5. All links

The information that each link stores contains the source address, the destination address, and the amount of remaining keys on the link. For example, given [src = 00: 00: 00: 00: 00: 00: 00 :01,outPort = 2, dst = 00: 00: 00: 00: 00: 00: 00: 02, inPort = 1, Qkey = 100], this means the switch named ID 1 is connected to port 1 of the switch named ID 2 through port 2 and there are still 100 kbits of keys on this link.

4 A routing algorithm for quantum cryptographic communication network

In the cryptography communication network, due to the existing conditions, the quantum key generation rate is relatively low, but a secure network requires massive keys. Thus, it is not feasible to consider only the number of links. So in addition to the link hops, we also use the number of available keys on the link as a routing condition[1][11].

4.1 Implementation steps of routing algorithm

Now that the key management layer has obtained the key's information of each link on the whole network, we can implement the routing based on the following steps:
1. First, the key management layer uses the Yen's algorithm (an extended version of the Dijkstra algorithm that solve the k shortest path problem) to select the k shortest path.
2. Then it traverse each path to learn the amount of keys on each path.
3. Now it compares the amount of keys of the bottleneck link on the path and removes the inappropriate paths that the amount of the available keys on their bottleneck link is lower than a certain threshold. The communication process of the service such as voice and video is considered to be bidirectional, and we can get the following equation:

$$V_A T = 2(V_K T + W) \tag{1}$$

Where V_A denotes the coding rate of the communication service, V_K is key rate, W denotes the demand for link keys Ideally. Taking into account the case of key loss, we set the link

key threshold to $1.2W$. T is communication time. We can adjust the threshold according to the values of V_K and V_A.

$$W = \frac{V_A T - 2V_k T}{2} \tag{2}$$

4. In the remaining paths, it selects the path with the least number of hops as the optimal choice.

Because we use the one-time-pad encryption scheme, the amount of available keys on *ith* link is related to the total number of keys generated, we denote it by S_i, and the length of each packet, denoted as Pj, through this link. The amount of the available keys on the link, denoted as *Ri*, is calculated as follows:

$$R_i = S_i - \sum_{j=1}^{N} P_j \tag{3}$$

where N denotes the number of packets that pass through the link.

Assume the total number of links that this path traverses is L, The amount of the available keys in the bottleneck link, denoted by m, can be expressed as

$$m=min\{R_1, R_2,..., R_L\} \tag{4}$$

4.2 Experimental simulation

Using the topology of figure 4 and our designed program, three alternative paths from h5 to h2 are generated.

In the quantum cryptography communication network, we refer to the coding rate of voice services and we can set V_A is 8kbit/s and V_K is 5kbit/s. Through the formula (2), we can get the 1.2W is 70kbit. So we modify the core code of floodlight to simulate the process of our algorithm.

Then let h5 continuously send UDP packets to h2, and we record the path was selected at different time as shown in Fig.6.

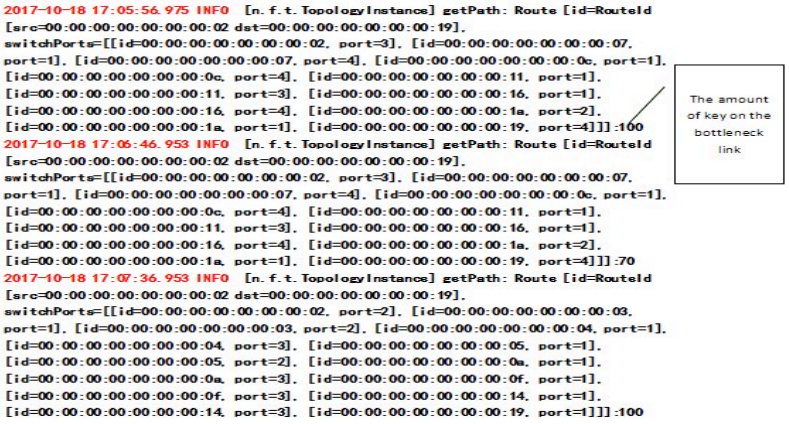

Fig. 6. Optimal path

The experimental results show the system automatically changes the route when the key value of bottleneck link of the first path is below the threshold. Experiments show that our algorithm is feasible.

5 Conclusion

The quantum key generated by QKD is a very valuable resource, and its management is of great significance.

This is the first time to integrate the idea of SDN into the quantum cryptography communication network, which is a quite reasonable innovation. In this paper, a quantum cryptography communication network model based on SDN is proposed to realize the flexible control of quantum key resources in the whole cryptography communication network and on this basis we propose a routing algorithm. Compared to other routing algorithms, the routing algorithm is more globally optimal.

SDN is one of the hot spots of the current network research. We will pay our attention on this domain constantly. We will study how to develop the flowtable, so that our quantum cryptography communication network model is more practical. And the number of switching nodes and host nodes in the actual network is much larger than the number of our simulation experiments, so we will expand our model for multi-controller mode. We believe that multiple controllers work together to manage the entire network and its control efficiency can increase significantly.

We will use further simulation experiments to demonstrate that quantum cryptography communication network that contains SDN thought has a great advantage in the management of keys and other network resources.

References

1. M. Li, “Stochastic routing in quantum cryptography communication network based on cognitive resources,” in The Ninth International Conference on Wireless Communications and Signal Processing, 2016.network based on cognitive resources,” in The Ninth International
2. M. M. K. Maurya A K, “A survey on software-defined network and openflow: From concept to implementation.,” IEEE Communication
3. K. Govindarajan, “Interoperability issue between ipv4 and ipv6 in openflow enabled network,” in 2014
4. V. R. Dasari1 and T. S. Humble2, “Openflow arbitrated programmable network channels for managing quantum metadata,” The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, vol. 14, pp. 1 – 11, 2016.
5. M. M. K. Maurya A K, “Two-way quantum communication: Generalization of secure quantum information exchange to quantum network[j].,”Pramana, pp. 515 – 526, 2016.
6. R. S. TS Humble, “Software-defined quantum communication systems,”
7. Optical Engineering, vol. 53, 2014.
8. V. R. D. . R. J. S. . R. P. . B. P. W. . T. S. Humble, “Programmable multi-node quantum network design and simulation,” Proceedings of the SPIE, vol. 9873, 2016.
9. T. S. Humble, “Quantum security for the physical layer,” The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, vol. 51, 2013.
10. R. V. M. J. Touch, “Designing quantum repeater networks,” IEEE Communications Magazine, vol. 51, pp. 64 – 71, 2013.
11. N. Y. Xiaoyuan Cao, “Dynamic openflow-controlled optical packet switching network,” Journal of Lightwave Technology, vol. 33, pp. 1500 – 1507, 2015.

12. T. L. W. M. K. N. RV Meter, T Satoh, “Path selection for quantum repeater networks,” Networking Science, pp. 82 – 95, 2013.