# Software Defined Quantum Key Distribution Network

Zhe Yan

School of Computer, National University of Defense Technology, Changsha, China

**Abstract:** Based on the analysis of the application scenarios of quantum key distribution(QKD), we will find it's necessary to develop QKD network, while point-to-point QKD hardly meets the requirements of real secret communication. To exceed the limits of the network layer protocols in the protocol stack of current QKD network, we propose applying the technology of software defined network to QKD network, building software defined quantum key distribution network, which is efficient in reducing the network's complexity, reducing the consuming of the local key, and realizing random routing.

## 1 Introduction

Quantum Key distribution (QKD) is the fastest developing quantum technology and most close to the practical application. Based on the analysis of the application scenarios of QKD, we will find it's necessary to develop QKD network, while point-to-point QKD hardly meets the requirements of real secret communication.

The DARPA Quantum Network pioneered the deployment of QKD in a field network[1]. The SECOQC QKD network was designed and implemented under the efforts of 41 research and industrial organizations[2]. In 2010, nine organizations from Japan and the EU participated in the Tokyo QKD Network operation[3].

There are three kinds of network model of QKD network: quantum switching network, quantum repeater network and trusted repeater network[4]. DARPA, SECOQC and Tokyo QKD Network all adopted the last model. Relay nodes divide the long distance link between Alice and Bob into several short links, with a hop-by-hop basis, encrypting and transmitting the session key, which are finally used for secure communication, with the local key that generated over short distance point-to-point QKD.

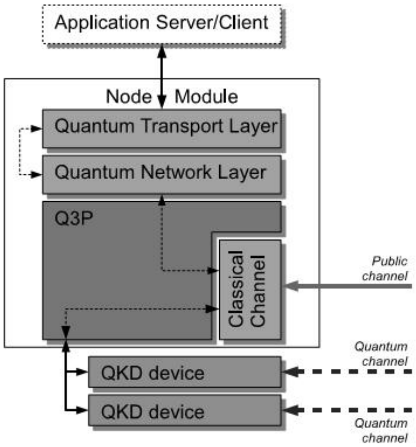

**Fig. 1** Node module of SECOQC[2]

Referred to the different layers of TCP/IP protocol stack, Fig.1 shows the division of current QKD network (SECOQC, for instance): physical layer, link layer, network layer, transport layer, application layer. In the SECOQC QKD network, network layer mainly have three functions[5]:

**Addressing:** SECOQC applied a addressing format and addressing scheme similar to IPv4.

**Route computation:** SECOQC adopted a heavily customized OSPFv2 protocol. Every node has to broadcast local link information to all nodes in the domain, Therefore, every node gets the global topology for route calculation.

**Forwarding:** forwarding module parsed the message header, and deliver the message to right out port according to the message's destination address and route table.

This architecture of network layer of current QKD network takes full advantages of the experience of the Internet. However, because of the limits of the Internet itself and QKD network's characters, some problems still exist in the network layer of SECOQC. First, large scale QKD network has numberless nodes and links. The flat addressing scheme and autonomous route scheme make the network more complicated. Second, link status information broadcasts ceaselessly with lots of local key consumed, because link information needs to broadcast to all nodes in the domain.

Software defined network (SDN) is the latest development of classical computer networks. Based on the idea of layering, SDN separates data and control. Data plane takes charge of forwarding and control plane takes charge of routing[6].

We propose applying SDN to QKD network, building software defined quantum key distribution network (SDQKDN), so as to solve the problems mentioned above.

# 2 Design of the SDQKDN

## 2.1 Network address

Firstly, we need to assign at least one address for every node in the network in order to identify the node uniquely. We adopted a addressing format and addressing scheme similar to IPv4, as SECOQC did.

The address is used not only as the node identifier but also as the address for classical channel. For instance, the address 10.0.0.10 identifies a node in the network and it's used for IP address in socket, too.

## 2.2 Architecture of the SDQKDN

Based on the current research on SDN and the requirements of QKD network, we presented the architecture of the SDQKDN as Fig.2.

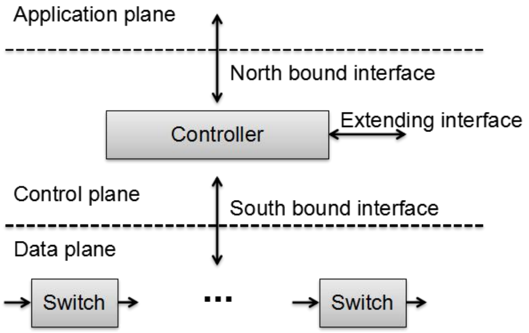

**Fig. 2** Architecture of the SDQKDN

SDQKDN includes three parts: data plane, control plane and application plane. SDQKDN switches deployed in relay node constitute data plane, and SDQKDN controllers compose control plane. Communication connections between data plane and control plane were established via south bound interfere, while connections between control plane and application plane via north bound interfere.

### 2.2.1 Data plane

In SDQKDN, data plane (switches) has two tasks:

**Link information collection:** there are lots of information about link status, including storage of local key, generation rate of local key, quantum bit error rate of local key, etc. These information related with route computation can be collected from key store module in Q3P[7] and sent to controller via south bound interfere.

**Session key forwarding:** switch maintains a flow table with table entries got from controller. When session key message arrives, switches parse the message header to get the message's destination address and look up flow table to search an out port for delivering the message.

### 2.2.2 Control plane

As with switches, SDQKDN control plane (controller) was also deployed in relay node, because data exchange between controller and its subordinate switches should be encrypted or authorized, too. Control plane has three tasks:

**Topology management:** controller gathered node and link information from switches and processed these information to build global topology, which would be the data support for route computation and users of application plane.

**Route management:** there are two means for generating flow table entry. The first way, controller could calculate basic table entries. The second way, application plane gets network topology via north bound interfere and calculates table entries with session requirements. Controller distributes these entries to all the switches on the data transfer path.

**Extending interfere:** hierarchical controller model realized layered network topology of QKD network logically. When nodes involved in a session go beyond the scope of a controller, this controller could submit the subnet's global topology and session request to a senior controller for solution.

## 3 Discussion

This paper concentrates on the network layer protocol in the protocol stack of trusted repeater QKD network. Analyzed the limits of current network layer protocols, we propose applying SDN technology to QKD network. There are mainly two benefits of this architecture:

Firstly, because of the difficulty to construct backbone in QKD network, current QKD network seems flatted. Hierarchical controller model constructs layered network topology that contributes to reducing the network complexity. What's more, controller-switch pattern makes the network administration more flexible and convenient.

Secondly, network topology won't change frequently, but link status information has to broadcast ceaselessly with lots of local key consumed. Link information broadcasts to all nodes with OSPFv2, while controller only with SDQKDN. The latter could reduce the consuming of the local key.

There are other advantages of SDQKDN: realizing random routing, integrating KMS (mentioned in the Tokyo QKD network) into SDQKDN controller, etc. To conclude, QKD network is very suitable for applying SDN technology.

[1] Elliott C, Pearson D, Pikalo O. Current status of the DARPA quantum network. Proc of Spie 2005, 5815: 138-149.

[2] Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, Boxleitner W, et al. The SECOQC quantum key distribution network in Vienna. New Journal of Physics 2009, 11(7): 075001.

[3] Sasaki M, ., Fujiwara M, ., Ishizuka H, ., Klaus W, ., Wakui K, ., Takeoka M, ., et al. Field test of quantum key distribution in the Tokyo QKD Network. Optics Express 2011, 19(11): 10387-10409.

[4] Elliott C. Building the quantum network. New Journal of Physics 2002, 4(1): 46.

[5] Dianati M, Alléaume R, Gagnaire M, Shen X. Architecture and protocols of the future European quantum key distribution network. Security and Communication Networks 2008, 1(1): 57-74.

[6] Mckeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, et al. OpenFlow: enabling innovation in campus networks. Acm Sigcomm Computer Communication Review 2008, 38(2): 69-74.

[7] Maurhart O. QKD networks based on Q3P. Springer Berlin Heidelberg, 2010.