Optical Fiber Technology 45 (2018) 195–200

Contents lists available at ScienceDirect

Optical Fiber Technology

journal homepage: www.elsevier.com/locate/yofte

A flexible key-updating method for software-defined optical networks secured by quantum key distribution

Hua Wang[a], Yongli Zhao[a,*], Yajie Li[a], Xiaosong Yu[a], Jie Zhang[a], Chuan Liu[b], Qi Shao[c]

[a] State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b] Global Energy Interconnection Research Institute Co., Ltd, Beijing, China
[c] State Grid Henan Information & Telecommunication Company, Henan, China

ARTICLE INFO

Keywords:
Software-defined optical network (SDON)
Security
Quantum key distribution (QKD)
Key update

ABSTRACT

Security threat is a challenging issue for data transmission in optical networks. Quantum key distribution (QKD) is a promising security solution to optical networks to provide secure keys. Meanwhile, key update is of importance to enhance the security of key in the networks. The previous update method is to provide a fixed key-updating period which has a strong regularity to be easily found. To enhance the security of data services, we proposed a quantum key-updating process by introducing the architecture of SDON secured by QKD. Then, a flexible quantum key-updating method (Flex-KUM) and a quantum key-updating algorithm based on Flex-KUM are designed in the comparison with the fixed method with different update periods. The results show that a higher level of security requires more updating keys, which leads to an increase in the blocking probability. Therefore, there is a trade-off between the enhanced security and resources.

1. Introduction

In recent years, optical network is widely recognized as an important infrastructure, which specifically includes WDM optical networks [1] and EON optical networks [2]. For the government, finance, and military fields, the security of optical networks is becoming more and more important [3]. Optical networks are vulnerable to many cyberattacks, such as eavesdropping, which may result in huge property damage or even casualties [4]. While data encryption technologies in optical networks can effectively solve this problem, the advent of quantum computer can make these encryption technologies easy to be broken [5]. Therefore, a new and promising solution is needed to overcome these threats.

Quantum key distribution (QKD) is a promising security solution to optical networks because it can provide secure keys [6]. Based on the physical properties of the quantum, it can provide theoretically unconditional security keys for users that separate two places [7]. Currently, studies have found that quantum can be transmitted in optical fibers or free-space links [8,9]. Due to its low attenuation and high immunity to interference, fiber is considered to be an excellent carrier [9]. WDM-QKD becomes an attractive way for its compatible with the transmission of quantum signal and classical optical signal by wavelength division multiplexing (WDM) technology in one common fiber [10]. For the application of QKD, some studies have successfully established small-scale experimental platforms, such as DARPA network [11], SECOQC network [12]. Based on the above researches, some studies use QKD to solve the security problem of optical networks. To solve the security problem of optical networks, Cao et al. [13] proposed a QKD over SDON architecture. Cao et al. [14] designed a resource allocation scheme for quantum keys in optical networks integrated with QKD. Furthermore, a SDN-based resource scheduling method is designed for quantum key to secure network function virtualization (NFV) in Ref. [15]. However, these studies only consider how to integrate QKD into optical networks.

However, there is a risk that keys will be leaked in the both sides of communication [16]. Similar to the Advanced Encryption Standard (AES), it is necessary to update the keys in the network in a certain time. Thus, quantum key-updating methods have been discussed in the optical networks secured by QKD. Cao et al. [14] proposed a static key update method to update keys in a fixed period in optical networks. However, update period of this fixed update method is simple and strong- regularity. Since the difficulty of the eavesdropper discovered the value of key-updating period will increase as the increased time complexity because update period changes dynamically. Therefore, we use key-updating period as another dimension for enhancing network security.

In this paper, we focus on the update period of quantum keys, where key is updated with a random period to enhance the security of data

* Corresponding author.
E-mail address: yonglizhao@bupt.edu.cn (Y. Zhao).

https://doi.org/10.1016/j.yofte.2018.07.005
Received 23 January 2018; Received in revised form 19 May 2018; Accepted 2 July 2018

services. In our proposed method, we designed a key-updating process in the architecture of SDON secured by QKD. Based on it, a flexible quantum key-updating method (Flex-KUM) is investigated to enhance the security of data services dynamically. Simulation results show that Flex-KUM can achieve better secure degree of key services compared to the fixed quantum key-updating method. In addition, increasing keys need to occupy more resources which are limited in the network. Thus, a trade-off between security and quantum resources is discussed in this paper.

The rest of this paper is organized as follows. In Section 2, we designed a key-updating process in the architecture of SDON secured by QKD. Section 3 describes a flexible quantum key-updating method (Flex-KUM), which is designed to enhance the security in the comparison with no updating method and fixed update method. A corresponding dynamical algorithm is proposed to update quantum keys with different update periods. The simulation results of the proposed algorithm are investigated in Section 4. Section 5 concludes this paper.

2. Key-updating process in SDON architecture secured by QKD

In this section, SDON architecture secured by quantum key distribution is introduced based on which an update process of keys services in this architecture is described to enhance the security of data services.

2.1. Network architecture

Quantum key distribution (QKD) can provide quantum keys for data services in optical networks, so it is necessary to consider the feasibility of QKD integration in optical networks. Since the fiber interferes little with attenuation, it is considered an excellent carrier for quantum signals. Due to compatibility with the transmission of quantum signals and classical optical signals, WDM-QKD becomes an attractive way, and the interval bandwidth of 200 GHz [17] is required between quantum channels and data channels (or between quantum channels and measurement base channels), as shown in Fig. 1(a). Then, the quantum communication device continuously performs a point-to-point QKD at the node to provide a key for the services in the data communication device, as shown in Fig. 1(b).

Similar to traditional SDON architecture in Refs. [18–20], the architecture of SDON secured by QKD consists of an application (APP) plane, SDON controller, QKD plane and data plane, as shown in Fig. 1 (c). The interface among the application plane, the control plane and the data plane are referred to as the Northbound interface and Southbound interface. Data communication is achieved through data communication devices in the data plane, and point-to-point QKD generates corresponding key services through quantum communication devices in the QKD plane. The key service is defined as the information transmitted in the QKD (for example, quantum key and measurement basis, etc.), which needs to occupy a certain number of data channels (DChs), quantum channels (QChs) and measurement base channels (MChs) to implement the key distribution. To clearly illustrate the update process, we draw these channels on each plane. The APP plane generates data service requests and confirms its security requirements. The SDON controller calculates update period according to the security requirements of the data service, then selects a path and allocates resources. The QKD plane continuously transmits and updates key services according to the configured update period. Take the communication between node 1 and node n as an example, specific process is as follows.

2.2. Key-updating process

Next, the key-updating process is shown by the labels in Fig. 1(b). Due to the limited QKD transmission distance, the end-to-end transmission of key services needs through many times point-to-point QKD. For example, QKD firstly performs between node 1 and node 2, and then between node 2 and node 3 to complete key distribution between node 1 and node 3. When the SDON controller receives a data service request that needs to be transmitted from node 1 to node n, specific updating process is as follows.

Step 1: APP plane generates a data service request and its security requirement, and sends them to controller.

Step 2: Controller calculates an update period according to the security requirement, selects a path and allocates DCh resources. Then, controller notifies corresponding nodes in data plane to establish communication channels.

Step 3: Point-to-point QKD performs between node 1 and node 2 to complete key distribution. According to QKD protocol (for example,

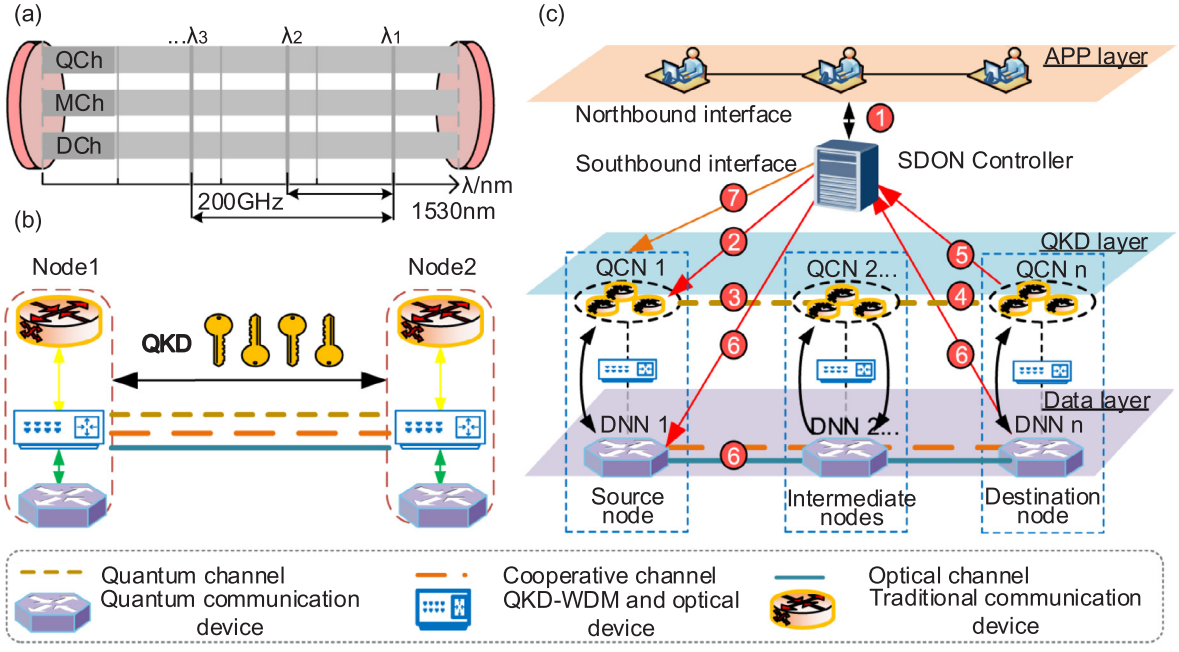

Fig. 1. SDON secured by QKD. (a) WDM-QKD in a fiber (b) point-to-point communication secured by QKD (c) key-updating process in SDON architecture secured by QKD.