Software Defined Quantum Key Distribution Networks

Yongli Zhao, Zhuangzhuang Ma, Hua Wang, Xiaosong Yu, and Jie Zhang
State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing, 100876, China
yonglizhao@bupt.edu.cn

Abstract: In the sight of quantum key distribution (QKD) development, this paper combines software defined networking (SDN) with QKD networks, introduces the architecture of software defined QKD networks (SD-QKDN), several related technologies and typical use cases.
OCIS codes: (060.4250) Networks; (060.4510) Optical communications.

1. Introduction

In recent years, information networks face security risks. As a promising technology, quantum key distribution (QKD) [1] has the advantage of theoretical "unconditional security" [2] and has gradually formed several small-scale QKD networks (QKDN) in practical area. With the increasing application requirements and further development, existing QKD networks requires a network control technique to effectively coordinate QKD resources on demand. Aiming at this problem, software-defined networking (SDN) [3] has gained consensus for its layered network division and the programmability of network functionalities. With the idea of SDN, QKDN [4, 5] can be achieved by the separation of network control and secret-key generation functions. To make QKDN flexible in practical use, this paper firstly discusses the architecture of SD-QKDN, and then analyzed four key technologies and three typical application scenarios.

2. Architecture of SD-QKDN

To better improve the openness and flexibility of QKDN, SD-QKDN architecture is described as follow. As shown in Figure 1, SD-QKDN architecture can be divided into four layers from top to bottom: application layer, control layer, QKD layer and data layer. Application layer generates security requests of services, according to which control layer can calculate QKD path in QKD layer and data layer, and allocate secret-key and wavelength resources. The QKD layer mainly distributes quantum keys for the data layer and control layer. The architecture utilizes the advantages of SDN to unify the optical network resources and the secret-key resources through northbound and southbound interfaces, thereby achieving unified control of the two types of resources, completing the efficient adaptation of the keys and services, and achieving the purpose of key distribution in the whole network.

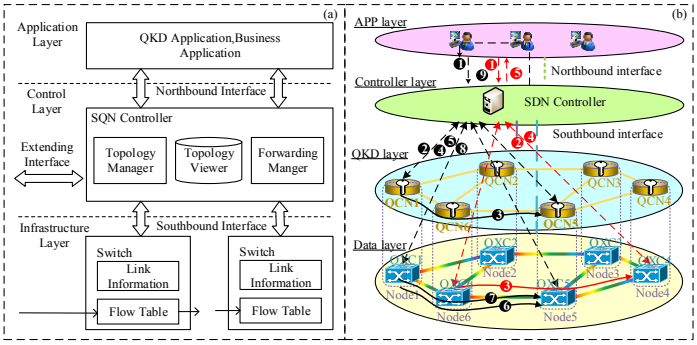


Fig. 1. SD-QKDN architecture

3. Key Technologies in SD-QKDN

3.1 SD-QKDN node constraint

In QKDN, the existing development trend caused by the compatibility of QKD devices and optical devices will directly affect the performances of the network. The most obvious influence is come from noises in physical fiber systems. For the QKD fiber system, the sources of noise interference are mainly divided into two categories: the noise generated by WDM devices and the noise caused by Raman scattering and four-wave mixing effects. To alleviate the impact caused by the above noises in QKDN, three basic constraints are proposed as shown in Figure 2 (a). (1) Ideally, when quantum optical signal and classical optical signal are transmitted together, the sum of their resources should not exceed the maximum number of spectrum resources on the physical link. (2) With the consideration of the influence of Raman scattering, four-wave mixing and isolation of wavelength division devices in the channel when the direction of quantum light should be the same as that of classical light. (3) Due to the

influence of Raman scattering, four-wave mixing, the channels used for QKD should be opposite to the direction of classical optical transceiver,

3.2 No-relay routing mechanism

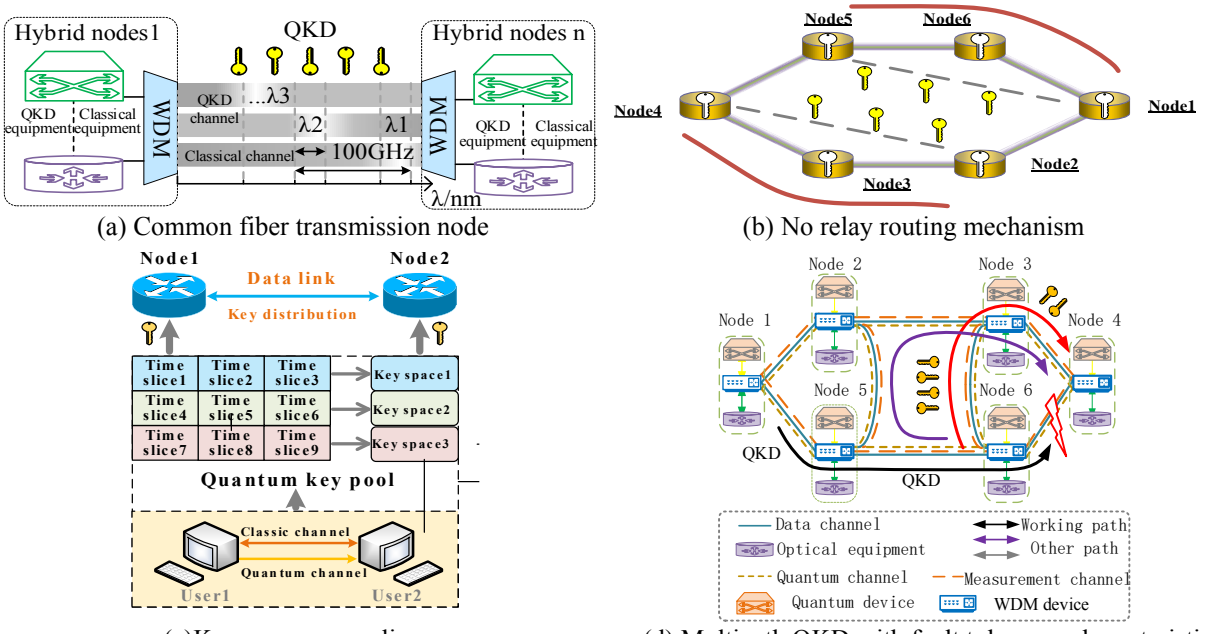
In QKDN, end-to-end key distribution can be realized with no-relay routing mechanism. This is because the performance parameters of QKD is different at various distances, such as the number of keys which can be regarded as fixed targets, and the appropriate path is calculated to generate the key to meet the requirements. At the same time, the QKD channel is divided into many slots, and the flexible allocation of these slots can be used as an adjustable factor to meet the demand. As shown in Figure 2 (b), for security requests arriving at different times, after obtaining the number of original and destination nodes and required keys, the comprehensive parameters can be used to calculate the appropriate routing. For multiple security requests arriving at the same time, multiple requests need to be considered to calculate and coordinate the appropriate routing to optimize the overall quality of service (QoS) of the network.

3.3 Resource pooling method

Quantum key pool (QKP) is an important component to store the secret keys generated in the network, which can be achieved by resource pooling method. The construction of QKP in QKDN can solve the problem of unsafe key distribution in existing technology. As shown in Figure 2 (c), the process of key generation can be considered as the process of pooling secret-key resources, which is also the process of decoupling key generation and key usage process. Based on these, firstly, the quantum node and link resources are integrated into a key pool. The quantum key is stored in the quantum key pool, and the quantum key pool is divided into multiple key spaces. Then, the key space is divided into several periodic time slices by using optical time division multiplexing technology. These time slices can provide periodic keys and update keys for multiple services, which can realize the one-to-many relationship between the key pool and the service to distribute keys on demand, and greatly improve the utilization of key resources.

3.4 Multipath key distribution method

Multi-path key distribution can provide a protection mechanism for key provisioning services. The core idea of the solution is to allocate multiple fiber resources on the working path for each key service, one as the working path and the other as the protection path. As shown in Figure 2 (d), when the security service request key pool allocates key resources for node 1 and node 4, three paths can be calculated: one working path is 1-5-6-4, and two protection paths are 1-2-3-4 and 1-2-5-6-4. When the working fiber receives a fault such as fiber cutoff, it will switch to multiple protection paths for key retransmission.



(a) Common fiber transmission node

(b) No relay routing mechanism

(c)Key resource pooling

(d) Multipath QKD with fault tolerance characteristics

Fig. 2. Key technologies in SD-QKDN

4. Typical Use Cases of SD-QKDN

4.1 QKD private networks

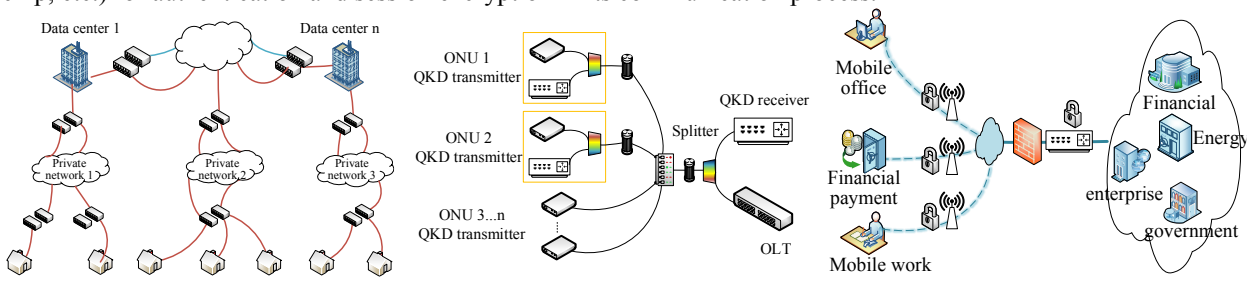
QKD can be used to protect the security of enterprise private network infrastructure and services in QKD private networks. Enterprises or government agencies usually require mandatory adoption of dedicated security systems. Currently, IPSec or TLS-based secure virtual private network (VPN) technology is commonly used to authenticate and encrypt traffic between data center and branch, and QKD link encryption machine can be combined with these technologies to satisfy the information encryption between enterprise network sites, as shown in Figure 3 (a).

4.2 Quantum secure access networks

QKD is expected to be integrated into passive optical network (PON) of telecommunication access network to ensure communication security in PON network. As shown in Figure 3 (b), each ONU receives all downlink signals of OLT. In this process, encryption measures can be used to prevent ONU from eavesdropping on unsuitable content. The current solution is to use shared symmetric keys to encrypt/decrypt, or asymmetric method and public key certificate scheme to distribute. It will be willing to see that through QKD system, secure key distribution can be carried out between OLT and ONU to realize the encrypted transmission of ONU user data.

4.3 QKD mobile terminal communication network

Security guarantee of mobile terminals has become one of the hot issues in nowadays. Using the unique advantages of QKD and combining with key distribution center, quantum key can be applied to mobile terminal side to protect end-to-end and end-to-server communication security. It also can be applied in mobile office, mobile payment, Internet of Things and other scenarios. As shown in Figure 3 (c), the secret keys generated in QKDN can help to secure the information with several terminal's secure storage media (such as SD card, SIM card, security chip, etc.) for authentication and session encryption in its communication process.



(a) private network (b) QKD access network (c) QKD Mobile terminal network

Fig. 3. Typical use cases of SD-QKDN

5. Conclusions

In summary, this paper introduces the architecture of SD-QKDN and four key technologies: QKDN node constraints, QKDN relay-free routing mechanism, QKDN resource pooling method and QKDN multi-path key distribution method, and finally analysis typical application scenarios, i.e., QKD private network, quantum secure access network and QKD mobile terminal communication network.

6. Acknowledgement

This work was supported in part by National Natural Science Foundation of China (NSFC) (61822105, 61571058, 61601052).

7. References

[1] Wang H, Zhao Y L, Yu X S, Ma Z Z, Wang J Q, Avishek N, Yi L T, Zhang J, "Protection Schemes for Key Services in Optical Networks Secured by Quantum Key Distribution (QKD)," Opt. Commun. Netw, 67–78(2018).

[2] Cao Y, Zhao Y L, Yu X S, Cheng L J, Li Z Q, Liu G J, Zhang J, "Experimental Demonstration of End-to-End Key on Demand Service Provisioning over Quantum Key Distribution Networks with Software Defined Networking," In Proceedings of the OFC, San Diego, CA, USA,3–7(2019).

[3] Cao Y, Zhao Y L, Colman-Meixner C, Yu X S, Zhang J, "Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)," Opt. Express, 25, 26453–26467(2017).

[4] Zhao Y L, Cao Y, Wang W, Wang H, Yu, X.S, Zhang J, Massimo T, Wu Y, Biswanath M, "Resource allocation in optical networks secured by quantum key distribution," IEEE Commun. Mag, 56, 130–137 (2018).