Research Paper

DOI: 10.19729/j.cnki.1673-5188.2018.03.009
http://kns.cnki.net/kcms/detail/34.1294.TN.20180904.1712.002.html, published online September 4, 2018

A Quantum Key Re-Transmission Mechanism for QKD-Based Optical Networks

WANG Hua[1], ZHAO Yongli[1], WANG Dajiang[2], WANG Jiayu[2], and WANG Zhenyu[2]

(1. State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, 100876, China;
2. Skill Transfer Management Department, ZTE Corporation, Beijing 100000, China)

Abstract

Due to the vulnerability of fibers in optical networks, physical-layer attacks targeting photon splitting, such as eavesdropping, can potentially lead to large information and revenue loss. To enhance the existing security approaches of optical networks, a new promising technology, quantum key distribution (QKD), can securely encrypt services in optical networks, which has been a hotspot of research in recent years for its characteristic that can let clients know whether information transmission has been eavesdropped or not. In this paper, we apply QKD to provide secret keys for optical networks and then introduce the architecture of QKD based optical network. As for the secret keys generated by QKD in optical networks, we propose a re-transmission mechanism by analyzing the security risks in QKD-based optical networks. Numerical results indicate that the proposed re-transmission mechanism can provide strong protection degree with enhanced attack protection. Finally, we illustrated some future challenges in QKD-based optical networks.

Keywords

optical networks; security; QKD; re-transmission

1 Introduction

The explosive growth of services has led to a growing demand for bandwidth and transmission quality, which poses a serious challenge to network operators. At the same time, operators need to manage both IP layer and optical layer in the optical networks, which results in a waste of time and energy overhead and rapidly increase in operating costs by repeating resource construction. The developed technology of IP over optical layer can solve this problem.

However, because optical network is a communication infrastructure to support people's daily life, it is widely recognized that the optical layer in IP over optical networks is crucial in supporting the rapidly growing traffic. Therefore, issues related to optical layer security become very important, which suffers more and more security incidents which are mainly by the method of eavesdropping information in optical networks to carry out harmful behavior. For instance, the world's largest bitmaker trading platform was attacked in 2014 and the loss was estimated about $467 million, which was caused by eavesdropping information in the fiber. Hence, it is crucial to solve the security problem of the optical layer, which also means the security problem in optical networks.

Caused by the weak defense of physical layer and the simplicity of logic layer in optical networks, services in transmission are vulnerable to security threats; the solution to this security issue depends on the encryption of services. Standard optical network encryption approaches typically utilize complex mathematical questions and decrypting them is not difficult but needs time only. This may be effective in the presence of failures under normal circumstances, but may fail to provide adequate protection for the services under deliberate eavesdropping.

To deal with this problem, an "absolutely safe" solution for the above problems in optical networks is quantum communication which could let the clients notice whether the quantum key has been eavesdropped based on the quantum mechanics inside itself [1]. The "absolutely safe" is guaranteed by quantum key distribution (QKD) over "one time padding" system [2]. Due to the above advantages, the topic about quantum communication in optical networks has been hot around the world. Quantum communication has been listed as the one of the top ten key technologies to promote the development of "13th five-year" plan in China. The National Institute of Standards Department of Defense and Technology of USA has regarded quantum as one of the key research directions. The Europe has invested billions of dollars in its quantum projects. Japan has proposed a long-term research strategy for quantum communication. The introduction of quantum communication into optical networks as a security support can effectively avoid the risk of unsafe communication and ensure the "absolute security" of optical networks, which has a very important innovative value and practical significance.

2 QKD Fundamentals

2.1 QKD Protocols and Networks

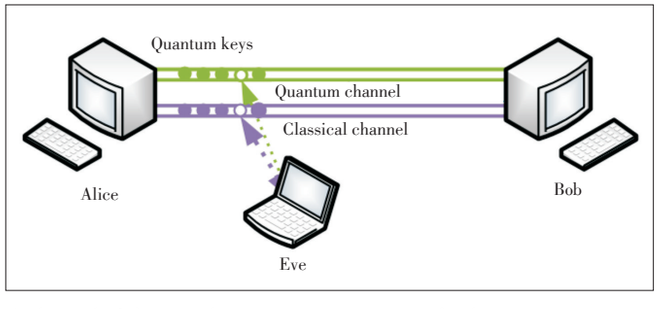
QKD is a process which enables both sides in communica-

This work has been supported in part by NSFC project (Grant No. 61571058 and 61601052), Science and Technology Project of State Grid Corporation of China: The Key Technology Research of Elastic Optical Network (Grant No. 526800160006), China Postdoctoral Science Foundation Project (2016M600970), and ZTE Industry-Academia-Research Cooperation Funds.

tion to share a secure key by encrypting and decrypting services, which needs corresponding protocols and networks to formulate the rules and realize the wide-spread confidential communication.

A QKD protocol is used to arrange the behavior of both sides in communication to achieve the proposal of security. The BB84 protocol is the first international quantum key distribution protocol, which has been proposed since 1984 to increase the safety of communication distance, improve the security rate and improve the real system security. **Fig. 1** shows the point-to-point quantum key communication procedure, where the sender (commonly known as Alice) and receiver (commonly known as Bob) use quantum channels to transmit quantum states, taking into account the possibility that both channels are eavesdropped by a third party (commonly known as Eve). Other related protocols include the B92 protocol, six-state protocol, and E91 protocol [3].

QKD networks refer to the operability among multiple nodes in secure communication. The quantum network of Defense Advanced Research Projects Agency (DARPA), an agency of the United States Department of Defense, uses multi-optical switches and trusted relays in the backbone to connect multiple subnets [4]. The Secure Communication Based on Quantum Cryptography (SECOQC) network in the Europe and the QKD network in Tokyo, Japan use the trusted relay to build quantum networks [5], [6]. Moreover, University of Science and Technology of China has designed a full-time all-quantum router based on the wave division multiplexer, and used it as the core technology to build the "four-node star" QKD network in Beijing, China and "multi-level" quantum government network in Wuhu, Anhui Province of China [7]–[9], which is in the forefront of the world. Shandong Institute of Quantum Science and Technology in China took the application demonstration of quantum communication integrated in optical networks in 2015, which passed the testing and achieved the QKD network under a multi-user environment. To promote the QKD as the core technology of quantum network construction, China launched the world's first quantum science experimental satellite "Micius" in 2017. Following it, a long-distance quantum communication backbone optical network in China is being completed between Beijing and Shanghai to achieve the backbone network QKD and promote wide area quantum communication [10].



▲Figure 1. Point-to-point quantum key communication procedure.

2.2 Key Technologies of QKD in Optical Networks

Nowadays, the main studies of quantum communication in optical networks are focused on the mixed transmission of quantum and classical light, deployment of quantum relay or trusted relay, quantum coding and quantum storage in optical networks, and other research directions. However, we mainly discuss the compatibility of quantum communication integrated with optical networks and the related transmission technology of mixing quantum signals and classical light.

The compatibility of quantum communication in classical optical networks is one of the crucial factors that directly affect the performance of quantum optical network and cost of network construction. The energy in optical pulse of a single photon (quantum key) transmitted in a QKD channel is about 1.28×10^{-19} J at 1550 nm. In previous experiments, QKD systems used a single mode fiber to realize the longest transmitted distance of QKD, which up to 250 km with ultra-low loss [11]. In the case of point-to-point QKD connection in fiber, quantum can reach Mbit/s level rate [12]. Because of the high cost of laying and leasing fiber, the way that both quantum and classical light are multiplexed and transmitted in a fiber can effective save cost and improve fiber utilization, which is significant for the development of quantum communication. For the same reason, the research in transmission of mixing QKD channels and classic channels in a common single fiber with wavelength division multiplexing (WDM) technology is gradually increasing. The transmission of combined QKD and services using WDM technology was first demonstrated in 1997 [13]. Subsequently, the quantum channel is accurate to O-band (1260 nm–1360 nm) to achieve confidential communication [14], [15].

In order to transmit weak quantum and dense classical light with WDM technology, we need solve two key problems: 1) Due to the large number of services, effective isolation is needed to prevent the quantum from being flooded by the classical light; 2) nonlinear noise is caused by the Raman scattering and the four-wave mixing effect, which would cause the quantum deteriorate seriously. Different solutions to the above problems have been proposed. A classical and quantum mixed transmit mechanism was proposed, which could effectively inhibit the four wavelengths and noisy filtering effect by non-uniform wavelength interval over C-band [16]. A multi-stage band-stop filter technique was developed then, which utilizes multi-stage filter to realize the effective isolation of quantum channel, synchronization channel and classical channel [17]. The wavelengths of quantum and synchronization signals are 1550.12 nm and 1556.55 nm, the quantum error rate is as low as 0.9% to 2%, which could achieve the optical transmission distance up to 45 km [18]. Classic channels and quantum channels cannot near the position of long wavelength was found, which could avoid the Raman noise, and working away from the optical fiber zero dispersion wavelength can effectively reduce the

generation of four-wave mixing effect.

3 Security Analysis of QKD in Practical Optical Networks

Today's optical networks provide suitable infrastructure for kinds of services ranging from government networks, financial networks, military networks, social networks to communicating or trade online networks, which are supposed to be protected by at least one quantum key according to the security requirements of users; one key can only be used once. Therefore, a large number of quantum keys are transmitted in the optical network for real-time protecting services. While the "unconditional security" of QKD was proven, several practical security concerns in QKD integrated in optical networks are still need to be solved for compatibility. We analyze this complex security issue in a systematic way with respect to quantum key transmission failure, eavesdropping, and authentication failure.

3.1 Quantum Key Transmission Failure

With the development of computer technology, security requirements of data service users are also increasing. Therefore, it is necessary to transmit a large number of quantum keys in a limited amount of resources in the optical network. If there is no resource in the network that can be provided for the quantum key, or if the quantum key is distributed at the receiver, we believe that the quantum key transmission fails once the quantum bit error rate is higher than a certain threshold.

3.2 The Security of Keys in Other Ways

The behavior of eavesdropping is inevitable, which is inherent to the attacks in optical networks that need to be protected using quantum. Because practical QKD devices are immature and fibers are vulnerable, the keys generated by QKD are still vulnerable to some attacks since keys still have the risk of leakage [19]. In order to prevent service leakage, they still need to be encrypted with the permitted conditions.

3.3 Quantum Key Authentication Failure

The quantum key is used for secure encryption of data information in multi-side quantum communication. The related protocols ensure a secure key reaches the receiver, while the identity of both sides in communication cannot be guaranteed and building a fade receiver could make the information eavesdropped. Thus, the communication sides need to be authenticated before the data transmission.

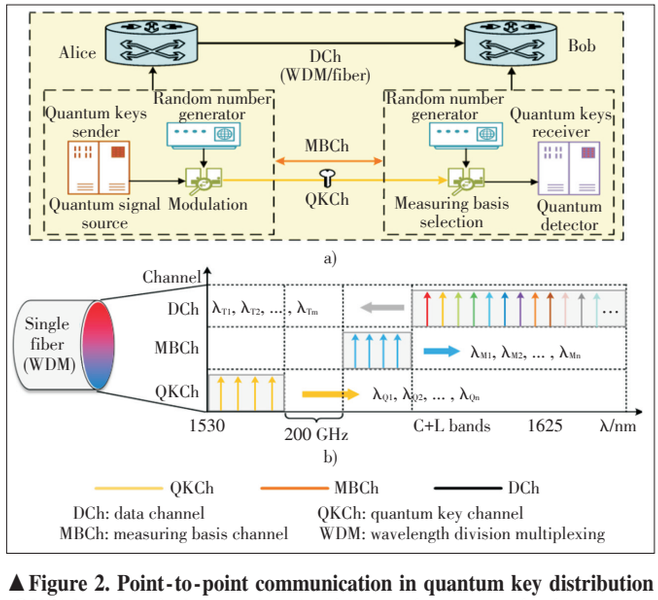
4 Quantum Key Re-Transmission Mechanism

4.1 Architecture of QKD-Based Optical Networks

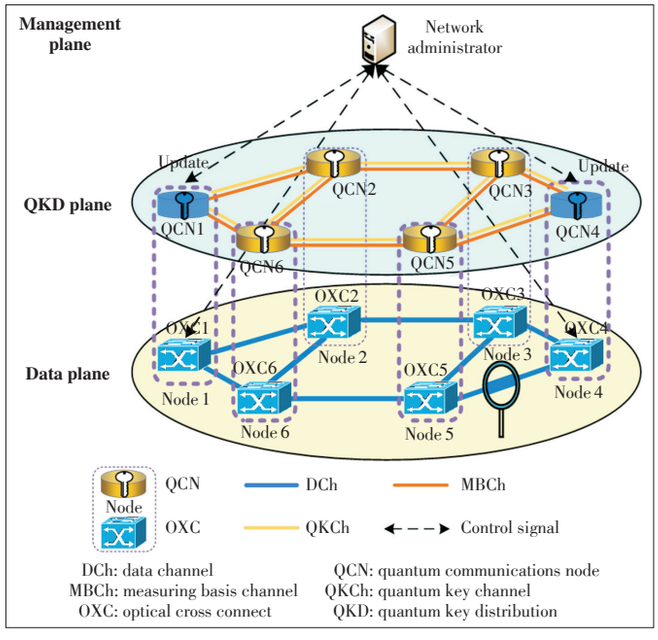
Optical networks are important infrastructure of communication systems. With the continuous improvement in flexibility and intelligence of optical networks, the concept of using quantum communication to enhance its security has been put forward [4]. Quantum keys are generated by QKD technology to encrypt the services, following which the network administrator selects paths and allocate resources for the keys.

The point-to-point communication in QKD-based optical networks is shown in **Fig. 2**. The architecture has the application plane, management plane, QKD plane and data plane from top to bottom. To realize point-to-point protection for services, QKD communication is realized by sharing a quantum key between quantum transmitter and receiver through quantum key channel (QKCh) and measurable basis channel (MBCh) (Fig. 2a). QKCh and MBCh can share the same fiber with data channel (DCh) over C-band (Fig. 2b) by WDM technology to save fiber resources and reduce costs [20]. Optical cross-connect devices (OXCs) are deployed at the data plane and QKD plane using trusted-nodes.

Fig. 3 shows the architecture of QKD-based optical networks. To realize end-to-end protection for services, secure communication requests are first generated from clients. Then this would be received by the management plane which is responsible for route forwarding and resource allocation at the QKD and data planes. The QKD plane is logically separated from the data plane but in the same physical entity. The QKD plane provides quantum keys to protect the services at the data plane, which includes the management of quantum keys and the service encryption process, such as update of quantum keys and the process of quantum key distribution. The management of quantum keys becomes flexible and intelligent for the network administrator, and the administrator is able to adaptively change the keys to effectively guarantee the whole net-



▲**Figure 2. Point-to-point communication in quantum key distribution (QKD) based optical networks: a) point-to-point communication system; b) wavelength allocation in fiber [21].**



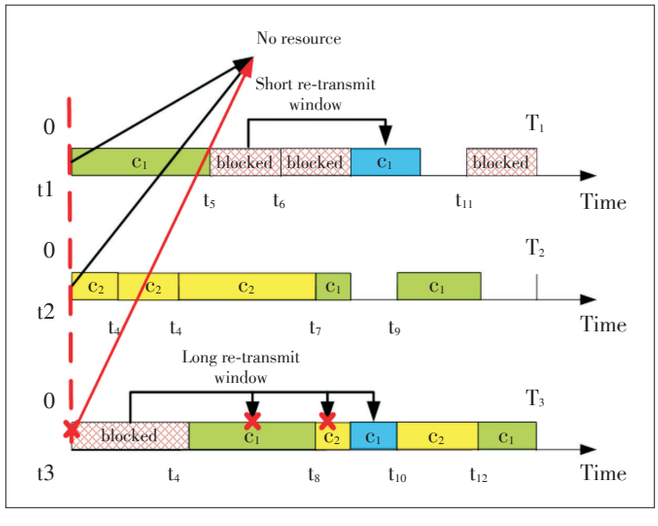
▲Figure 3. Architecture of QKD-based optical networks.

work security.

4.2 Quantum Key Re-Transmission Mechanism

In response to the above analysis, we propose a quantum key re-transmission mechanism, analogous to the Advanced Encryption Standard (AES) in classical optical networks [22].

As shown in **Fig. 4** and **Algorithm 1**, the mechanism is a re-transmission process of failed quantum keys. As there are lots of services transmitted in a QKD-based optical network, the start of re-transmission of the failed quantum key is always caused by the limited optical network resource. When one of these cases occurs, the failed quantum key needs to formulate a re-transmission time window, which could try many times within a range. The re-transmission time window depends on the security degree required by users. A high secure degree service needs a large re-transmission time window to try many times for safely reaching the receiver, just like the third axis. A low secure degree service re-transmits within a short time window. For example, there are six wavelengths in one fiber used for services, quantum keys and measurable basis information, respectively. When all the quantum key channels are occupied, the quantum keys need wait a certain time to re-transmit.



▲Figure 4. Re-transmission of quantum keys.

Algorithm 1: quantum key re-transmission

```
1. For each quantum key {
2.   While (failed quantum key been detected) {
3.       Select random distribution;
4.       Set the range of Δt ;
5.       Do {
6.          Generate t_ri in the range of time window
7.          utilizing the distribution;
8.       } While ( t_ri < T_ei ) t_si
9.   }
10.  While ( clock comes to t_ri ) {
11.         Compute one path d utilizing Dijkstra
12.         algorithm;
13.         If d ≠∅ Ø , Then First Fit algorithm for
14.                  time-slot assignment;
15.         Else the quantum key failed to transmit;
16.  }
17. }
```

We give specific quantum key re-transmission algorithms for users in need of different secure requirements. A quantum key in the algorithm is denoted as q_r $(s, d, t_s, t_h, t_r, \Delta t)$, where u is the number of quantum keys, s and d represent sources and destination nodes, t_s and t_h are its start time and hold time respectively, and Δt is the time window width. The arrival time of each update key is denoted as t_{si}, which should be generated before the leaves of data service T_{ei}. The hold time of each re-transmission quantum key is a fixed value of 1s. Firstly, once a quantum key transmission failure is detected, the secure degree of the service is judged and a re-transmission time window is set. If the secure requirement is in a high degree, we set a long range for the time window and vice versa. The range values are designed according to the simulation results. Then, when the clock goes to t_{si}, the network administrator computes one shortest path among several available paths by the Dijkstra algorithm with the same source node and destination node with the services. If there is no available path or time slot, this quantum key is failed to be transmitted and then would be thrown away.

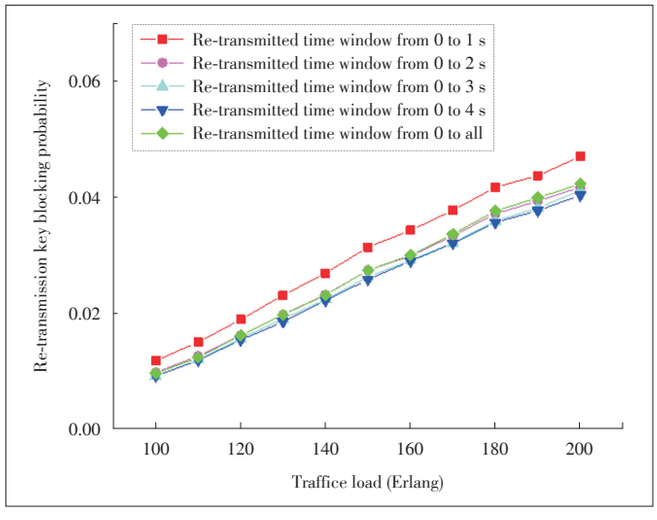
4.3 Simulation Results

Simulations were conducted to evaluate the proposed mecha-

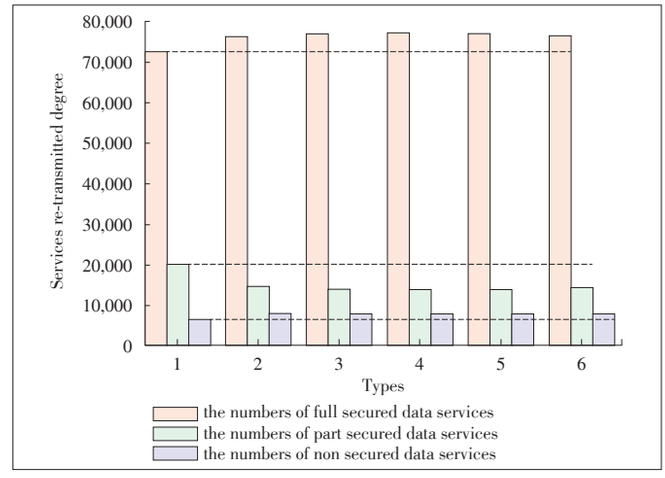
nism and ensure the feasibility of the re-transmission mechanism. In the simulation, the topology is a national science fund network (NSFNET) with 14 nodes and 21 links. The number of services is 100,000. The wavelength numbers of DCh, QKCh and MBCh are set as 28, 4, and 4, respectively. The simulations were carried out in the software virtual studio that is based on C++ language. We studied the performance of QKD-based optical networks in terms of blocking probability, resource utilization probability, re- transmission protection degree and re-transmission successful probability.

We simulated re-transmission of quantum keys random generated from different size time windows (**Fig. 5**). The quantum key was re-tried from the current failure time, and the time window is increased by 1 s each time until the data service transmission time ends. It can be seen that the blocking rate of a re-transmission quantum key becomes stable gradually as the traffic load increases. We found that larger key re-transmission time windows could result in lower blocking probability by comparing the time windows with different sizes. This is because more time is given to make the failed quantum key have more chances to try re-transmission. This could increase the security of data services.

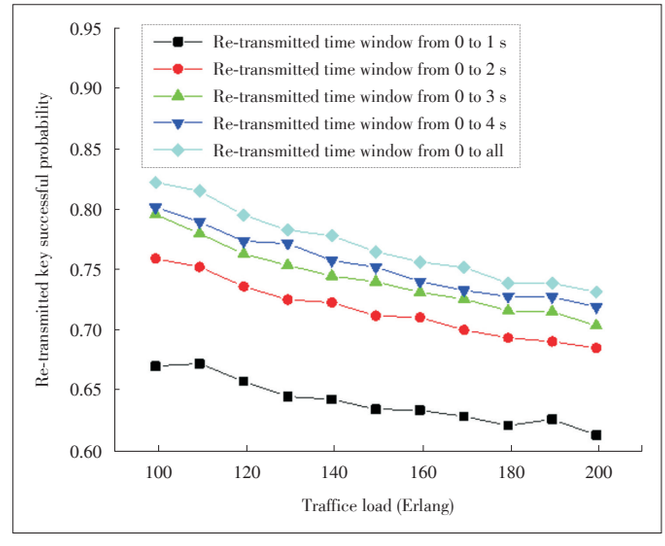
Fig. 6 shows the protection degrees of data services after re-transmission compared with no re-transmission. The abscissa indicates the types of re-transmission time window in the order which are no re-transmission (type 1), [0, 1] (type 2), [0, 2] (type 3), [0, 3] (type 4), [0, 4] (type 5), [0, all] (type 6). The re-transmission has a certain increase in full-protect data services which are suitable for the high security level services compared with no re-transmission. The number of part-protect data services after re-transmission is reduced while the number of none-protect data services is slightly higher. The overall security level of the full-protect and part-protect data services is increased compared to the services with no re-transmission.



▲**Figure 5. Re-transmission key blocking probability in time windows with different sizes.**



▲**Figure 6. Services re-transmitted protection degree.**



▲**Figure 7. Re-transmit quantum key successful probability.**

The successful probability of key re-transmission in different sizes of time window is shown in **Fig. 7**. With the increase in traffic load (the density of data services), the overall trend of successful re-transmission is gradually small. The higher successful re-transmission probability is always with bigger time windows, which could reduce the blocking probability in a big degree (Fig. 4) to enhance the network security. Therefore, bigger re-transmission time windows can result in lower blocking probability, higher resource utilization and bigger numbers of successful re-transmission.

5 Main Research Challenges

With optical networks becoming more virtualized and intelligent, they are facing with various security risks. For these security problems, quantum communication can provide a reliable and secure scheme for optical networks, helping guarantee the

backbone security of telecommunication networks and reduce the complexity of management. QKD-based optical networks are developing from point-to-point application to multi-node application. However, further research is needed, especially on the important issues shown in **Fig. 8**.

5.1 Quantum Key Management

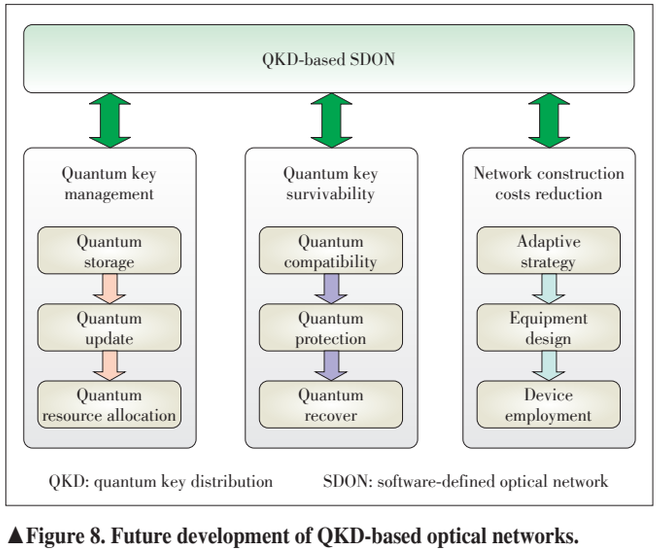
In recent years, quantum communication in optical networks has made great progress and entered the trial stage, in which the quantum nodes achieve receive and forwarding function both for quantum and classical light signals. It has become a consensus that quantum can be used for the medium that carries critical information, so the management of quantum keys has attracted much research attention because it is the basis for secure optical networks. Storing quantum keys at a node, updating quantum keys to ensure key security, and allocating resources for a large number of quantum keys are hot topics in the research of quantum key management.

5.2 Quantum Key Survivability

Survivability is an issue every network has to take into consideration, and QKD-based optical networks are no exception. It also means the disaster resistance of quantum keys in the network. In order to achieve the protection of services in optical networks, we should study protection and recovery measures of QKD-based optical networks, as well as the collaborative protection of quantum keys and services.

5.3 Network Construction Cost Reduction

Cost reduction plays a decisive role in the development and practical application of QKD-based optical networks. The high cost of network construction is always caused by the high cost of hardware equipment. The transmission of quantum combined with classic signal can not only ensure "absolute security" of services in optical networks, but also help to reduce the laying cost of fiber and that of its management and maintenance. The following issues are crucial for the cost reduction: how to select wavelength for quantum keys to reduce crosstalk with classical channels; how to make a long-distance safe transmission for reducing the use of hardware devices; how to deploy hardware devices at a minimum cost.



▲**Figure 8. Future development of QKD-based optical networks.**

6 Conclusions

With the development of quantum networks in metro areas, quantum communication is becoming a key technology to support optical security in the future. In this paper, we describe quantum communication as part of a secure communications solution, and specifically introduce the architecture of QKD-based optical networks for flexibly and dynamically protecting services. A more secure quantum key re-transmission mechanism is proposed to solve the security risk issue in QKD-based optical networks. The numerical simulation results show the good performance of the mechanism. Our future work will focus on quantum management, quantum survivability, and the cost reduction of network construction in QKD-based optical networks.

References

[1] D. J. Griffiths, *Introduction to Quantum Mechanics*. Cambridge, England: Cambridge University Press, 2016.
[2] S. S. Kute and G. C. Desai, "Quantum cryptography: a review," *Indian Journal of Science and Technology*, vol. 10, no. 3, 2017. doi: 10.17485/ijst/2017/v10i3/110635.
[3] W. K. Hong, M. O. Foong, and J. T. Low, "Challenges in quantum key distribution: a review," in *Proc. ACM 4th International Conference on Information and Network Security*, Kuala Lumpur, Malaysia, 2016, pp. 29–33.
[4] C. Elliott, A. Colvin, D. Pearson, et al., "Current status of the DARPA quantum network," in *Proc. SPIE 5815, Quantum Information and Computation III*, Orlando, USA, 2005, pp. 138–149. doi: 10.1117/12.606489.
[5] M. Peev, C. Pacher, R. Alléaume, et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, article no. 075001, Jul. 2009. doi: 10.1088/1367-2630/11/7/075001.
[6] M. Sasaki, M. Fujiwara, H. Ishizuka, et al., "Field test of quantum key distribution in the Tokyo QKD network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011. doi: 10.1364/OE.19.010387.
[7] S. Aleksic, D. Winkler, G. Franzi, et al., "Quantum key distribution over optical access networks," in *NOC/OC&I*, Graz, Austria, 2013, pp. 11–18. doi: 10.1109/NOC-OCI.2013.6582861.
[8] F. X. Xu, W. Chen, S. Wang, et al., "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chinese Science Bulletin*, vol. 54, no. 17, pp. 2991–2997, Sept. 2009. doi: 10.1007/s11434-009-0526-3.
[9] S. Wang W. Chen, Z.-Q. Yin, et al, "Field test of wavelength-saving quantum key distribution network," *Optics Letters*, vol. 35, no. 14, pp. 2454–2456, Jul. 2010. doi: 10.1364/OL.35.002454.
[10] S. Wang, W. Chen, Z.-Q. Yin, et al, "Field and long-term demonstration of a wide area quantum key distribution network," *Optics Express*, vol. 22, no. 18, pp. 21739–21756, Sept. 2014. doi: 10.1364/OE.22.021739.
[11] S. Wang, W. Chen, J.-F. Guo, et al, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Optics Letters*, vol. 37, no. 6, pp. 1008–1010, Mar. 2012. doi: 10.1364/OL.37.001008.
[12] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous operation of high bit rate quantum key distribution," *Applied Physics Letters*, vol. 96, no. 16, Mar. 2010. doi: 10.1063/1.3385293.
[13] D. P. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fiber using wavelength-division multiplexing," *Electronics Letters*, vol. 33, no. 3, pp. 188–190, Jan. 1997.

[14] J. R. Runser, T. E. Chapuran, P. Toliver, et al., "Demonstration of 1.3 μm quantum key distribution (QKD) compatibility with 1.5 μm metropolitan wavelength division multiplexed (WDM) systems," in *OFC/NFOEC*, Anaheim, USA, 2005.
[15] N. I. Nweke, R. J. Runser, S. R. McNown, et al., "EDFA bypass and filtering architecture enabling QKD+WDM coexistence on mid-span amplified links," in *Conference on Lasers and Electro-Optics/Quantum Electronics and Laser Science Conference*, Long Beach, USA, 2006.
[16] L. He, J. Niu, Y. Sun, and Y. Ji, "The four wave mixing effects in quantum key distribution based on conventional WDM network," in *12th International Conference on Optical Internet*, Jeju, South Korea, 2014.
[17] L. Wang, L.-K. Chen, L. Ju, et al., "Experimental multiplexing of quantum key distribution with classical optical communication," *Applied Physics Letters*, vol. 106, no. 8, Feb. 2015. doi: 10.1063/1.4913483.
[18] T. F. da Silva, G. B. Xavier, G. P. Temporao, et al., "Impact of raman scattered noise from multiple telecom channels on fiber-optic quantum key distribution systems," *Journal of Lightwave Technology*, vol. 32, no. 13, pp. 2332–2339, Jul. 2014. doi: 10.1109/JLT.2014.2322108.
[19] H. Wang, Y. Zhao, Y. Li, et al., "A flexible key update method for software-defined optical networks (SDON) secured by quantum key distribution," *Optical Fiber Technology*, vol. 45, pp. 195–200, Nov. 2018. doi: 10.1016/j.yofte.2018.07.005.
[20] I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10Gb/s WDM-PON," *Optics Express*, vol. 18, no. 9, pp. 9600–9612, 2010. doi: 10.1364/OE.18.009600.
[21] Y. Cao, Y. Zhao, X. Yu, et al., "Resource allocation in software-defined optical networks secured by quantum key distribution," in 2017 Opto-Electronics and Communications Conference (OECC) and Photonics Global Conference (PGC), Singapore, Singapore, 2017. doi: 10.1109/OECC.2017.8114769.
[22] F. P. Miller, A. F. Vandome, and J. McBrewster, *Advanced Encryption Standard*. South San Francisco, USA: Alpha Press, 2009.

Manuscript received: 2017-11-03

Biographies

WANG Hua (Whua@bupt.edu.cn) is currently working toward her Ph.D. degree in information and communications engineering at Beijing University of Posts and Telecommunications (BUPT), China. Her research interests include software defined optical networking and quantum communication.

ZHAO Yongli (yonglizhao@bupt.edu.cn) is currently an associate professor of the Institute of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications (BUPT), China. He received the B.S. degree in communication engineering and Ph.D. degree in electromagnetic field and microwave technology from BUPT. During Jan. 2016 to Jan. 2017, he was a visiting associate professor at UC Davis, USA. He has published more than 300 international journal and conference papers. Since 2015, he has become a senior member of IEEE. His research focuses on software defined optical networking, elastic optical networks, datacenter networking, and optical network security.

WANG Dajiang (wang.dajiang@zte.com.cn) is an experienced senior engineer and product planning manager of intelligent optical networks with ZTE Corporation. With 12 years of R&D experience in the intelligent optical network field, he has many optical-oriented SDN patents and was the core researcher of two "863" national scientific research projects of China.

WANG Jiayu (Wang.jiayu@zte.com.cn) is an experienced senior engineer and product planning manager of intelligent optical networks with ZTE Corporation. His research interest is intelligent optical networking.

WANG Zhenyu (Wang.zhenyu@zte.com.cn) is an experienced senior engineer and product planning manager of intelligent optical networks with ZTE Corporation. His research interest is intelligent optical networking.