Resource Allocation in Optical Networks Secured by Quantum Key Distribution

Yongli Zhao, Yuan Cao, Wei Wang, Hua Wang, Xiaosong Yu, Jie Zhang, Beijing University of Posts and Telecommunications, Beijing, China

Massimo Tornatore, Politecnico di Milano, Milan, Italy

Yu Wu, Biswanath Mukherjee, University of California, Davis, CA, USA

Abstract

Optical-network security is attracting increasing research attention, as loss of confidentiality of data transferred through an optical network could impact a huge number of users and services. Data encryption is an effective way to enhance optical network security. In particular, quantum key distribution (QKD) is being investigated as a secure mechanism to provide keys for data encryption at the end-points of an optical network. In a QKD-enabled optical network, apart from traditional data channels (TDChs), two additional channels, called quantum signal channels (QSChs) and public interaction channels (PIChs), are required to support the secure key synchronization. How to allocate network resources to QSChs, PIChs, and TDChs is emerging as a novel problem for the design of a security-guaranteed optical network. This article addresses the resource-allocation problem in optical networks secured by QKD. We first discuss a possible architecture for a QKD-enabled optical network, where a software-defined networking (SDN) controller is in charge of allocating the three types of channels (TDCh, QSCh, and PICh) over different wavelengths exploiting wavelength-division multiplexing (WDM). To save wavelength resources, we propose to adopt optical time-division multiplexing (OTDM) to allocate multiple QSChs and PIChs over the same wavelength. A routing, wavelength, and time-slot assignment (RWTA) algorithm is designed to allocate wavelength and time-slot resources for the three types of channels. Different security levels are included in the RWTA algorithm by considering different key-updating periods (i.e., the period after which the secure key between two end-points has to be updated). Illustrative simulation results show the effects of different security-level configuration schemes on resource allocation.

1. Introduction

Optical networks today represent a fundamental infrastructure for data transport in the Internet, with more than two billion kilometers of fibers deployed globally [1]. Fiber transmission in optical networks has been traditionally considered as a very secure communication platform, due to the inherent isolation of the optical signal inside the fiber medium (as opposed to wireless communication). Yet, over the past decade, several incidents have shaken this confidence. As an example, only in 2015, there were 16 known attacks on fiber-optic cables just in the San Francisco area; and, in several other cases, confidentiality of data transferred through an optical network is suffering from increased eavesdropping and interception [2]. Thus, implementation of security countermeasures directly at the optical layer is gaining importance.

Data encryption is an effective way to enhance communication security, as it prevents eavesdroppers to access the data unless they possess the encryption key. Several architectures that enable fast encryption in the optical domain have been proposed [3]; a commonly-used and fast data encryption method is the advanced encryption standard (AES) algorithm, whose encryption efficiency [4] makes it suitable for high-bit-rate optical networks. However, the security of current key-distribution techniques relies on their computational complexity, and the emergence of high-performance quantum computers will render most of today's encryption insecure [5].

Quantum key distribution (QKD) represents a future-proof solution to guarantee secure key distribution as it relies on quantum mechanics. The basic principles of quantum mechanics, e.g., quantum no-cloning theorem (i.e., an unknown quantum state cannot be copied) and Heisenberg uncertainty principle (i.e., no measurement by an eavesdropper can determine the value of both observables simultaneously) [6], can be used to prove that two remote end-points of an optical link can generate a shared random secure key known only to them by using specific quantum-communication protocols, such as BB84 proposed by IBM in 1984 [7]. Such a shared random secure key can then be used to encrypt the messages exchanged between the two end-points. The most important and unique feature of QKD is that the two communicating end-points are able to detect the presence of any third party trying to gain knowledge of the key, and this feature can significantly enhance the security of the key-distribution system.

For each optical connection to be established in the network, in addition to the traditional data channel (TDCh), QKD requires a quantum-signal channel (QSCh) and a public-interaction channel (PICh) for secure key synchronization [8]. Until now, researchers have tried to verify QKD's practicality in existing optical networks by testing quantum-signal transmission and secure key generation rate over different fiber spectrum areas [9-11], showing, e.g., that best transmission performance of QSCh is achieved in the C-band [10]; and that, to reduce the negative impact of physical-layer impairments, such as Raman scattering and four-wave-mixing, QSCh should be located at the highest frequency, and a large guard band, e.g., 200 GHz, should be reserved between QSCh and PICh [11]. So far, no studies have appeared on the networking aspects and algorithmic solutions related to QSCh and PICh allocation in the fiber spectrum. Using wavelength-division multiplexing (WDM), QSChs and PIChs can share the same fiber with traditional data channel (TDCh) to conserve fiber resources in optical networks. Since fiber spectral resources are finite (and precious, especially in the long haul), novel strategies for effective resource utilization in QKD-enabled optical networks are necessary.

In this article, we discuss the resource-allocation problem that arises when jointly serving the aforementioned three types of channels, and we propose an effective algorithmic solution to the problem. The contributions of this article are three-fold: 1) We illustrate a QKD-enabled optical network architecture, in which control plane is realized by using software-defined networking (SDN), and the three types of channels are configured by an SDN controller over different wavelengths. 2) We introduce the concept of different security levels, associated to different key-updating periods in QKD-enabled optical networks, and study the impact of two different configuration schemes for the key-updating periods. 3) We propose a novel routing, wavelength, and time-slot assignment (RWTA) algorithm to allocate resources for the three types of channels, and evaluate the benefits of RWTA over different scenarios, e.g., different key-updating periods and different configuration schemes of security levels.

2. Resource Allocation Problem in QKD-Enabled Optical Networks

2.1 Point-to-point QKD mechanism

To describe the basic idea of QKD, Fig. 1 shows the point-to-point QKD system for data encryption and decryption based on the most-widely-used QKD protocol, i.e., BB84 [7]. Note that, in long-distance networks, BB84 should be implemented based on a polarization-coding scheme combined with a decoy method, and in our system model, we assume that vacuum states are adopted as decoy states (for more information about physical-layer issues of QKD, as decoy and vacuum states, please refer to [9]). An example of the procedure to establish a secure optical channel with QKD is reported in Fig. 1: ① QSS (quantum signal source) transmits single photons to PF_1 (polarization filter), and RNG_1 (random number generator) generates random binary bits, e.g., 100110, to PF_1. ② A string of single photons passes through PF_1, where each photon can be polarized in one of four states: vertical ($V \rightarrow 1_+$), horizontal ($H \rightarrow 0_+$), and diagonal ($+45° \rightarrow 1_\times$ and $-45° \rightarrow 0_\times$), according to the generated random bit (i.e., either 1 or 0) and measuring-basis (i.e., either rectilinear (+) or diagonal (×)). The polarized single photons (called quantum signals) encoded with the random binary bits are also called quantum bits (qubits). ③ Alice sends qubits to Bob via QSCh, while PICh is used for clock synchronization of qubits. ④ After transmission, each qubit will be detected at PF_2 using a randomly-selected measuring-basis (generated by RNG_2). ⑤ QD (quantum detector) detects the qubits from PF_2 and decodes them to binary bits. ⑥ Bob sends his selected measuring-basis to Alice via PICh. ⑦ Alice confirms the correct measuring-basis via PICh to Bob. ⑧ Bob discards the bits which correspond to the unmatched measuring basis, and filters the final secure keys out after error correction, privacy amplification, and authentication via PICh [7]. ⑨ Alice uses the secure keys obtained as described above to encrypt data. ⑩ Alice transports encrypted data to Bob via TDCh. ⑪ Bob uses the shared keys from quantum receiver to decrypt data.

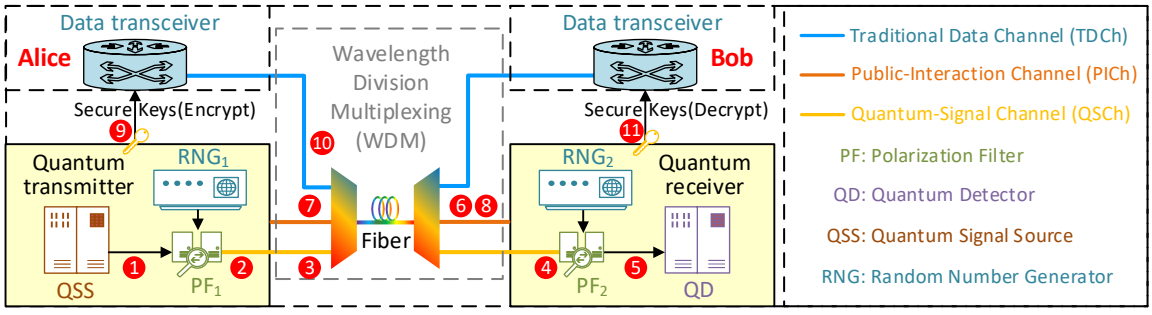

Figure 1. *Point-to-point QKD system for data encryption and decryption.*

Based on this mechanism, Alice and Bob can share a series of secure keys (e.g., keys with a length of 256 bits as required in AES) via QSCh and PICh. The key-synchronization process between Alice and Bob is described by phases ①→⑧, while the data encryption, transmission, and decryption process secured by QKD is described by phases ⑨→⑪. Note that the duration of the key-synchronization process is influenced by qubit transmission rate, link distance, and loss, but we can safely assume that, in a stable scenario, a key with fixed size can be successfully synchronized within a pre-determined maximal interval of time. Hereafter, this fixed period of time is named key-synchronization time, which includes the time for channel estimation and calibration, qubits transmission, switching, measuring-basis comparison, error correction, privacy amplification, and authentication.

2.2 QKD-enabled optical network architecture

To integrate QKD into existing optical networks, Fig. 2 shows the proposed QKD-enabled optical network architecture. It consists of four planes: application (App) plane, control plane, QKD plane, and data plane in top-down order. The application plane generates connection requests. Control plane is implemented using an SDN controller, and is in charge of resource management and allocation for QKD plane and data plane. Introducing SDN is beneficial to manage the entire network's resources via logically-centralized control. QKD plane and data plane share fiber spectrum resources using WDM technology to construct QSCh, PICh, and TDCh. A possible distribution of these three types of channels in the fiber C-band is shown in Fig. 2. Note that PICh belongs to the data plane together with TDCh because it can use the general transmitter and receiver. Quantum communication node (QCN) is defined as a network node with quantum-signal sending, receiving, and switching functions that can be realized based on the existing technologies for quantum transmitters, receivers, and switches [12]. A QCN and an optical cross connect (OXC) are physically co-located at one node.

Connection requests, with or without security requirements, are generated in the application plane. For example, as soon as a connection request from Node 1 to Node 5 is generated with security requirement, the SDN controller computes and allocates resources for TDCh, PICh, and QSCh (i.e., black solid line). In contract, the connection request from Node 6 to Node 4 without security requirement is served only by TDCh in the data plane (i.e., red solid line). The signaling procedures for configuration of these two requests are delineated in Fig. 2, as black and red dashed lines, respectively. For the connection request with security requirement, steps 2 to 4 complete the construction of QSCh and PICh for secure key synchronization, and steps 5 to 7 complete the construction of TDCh. Steps 1 and 8 are the connection request and confirmation.

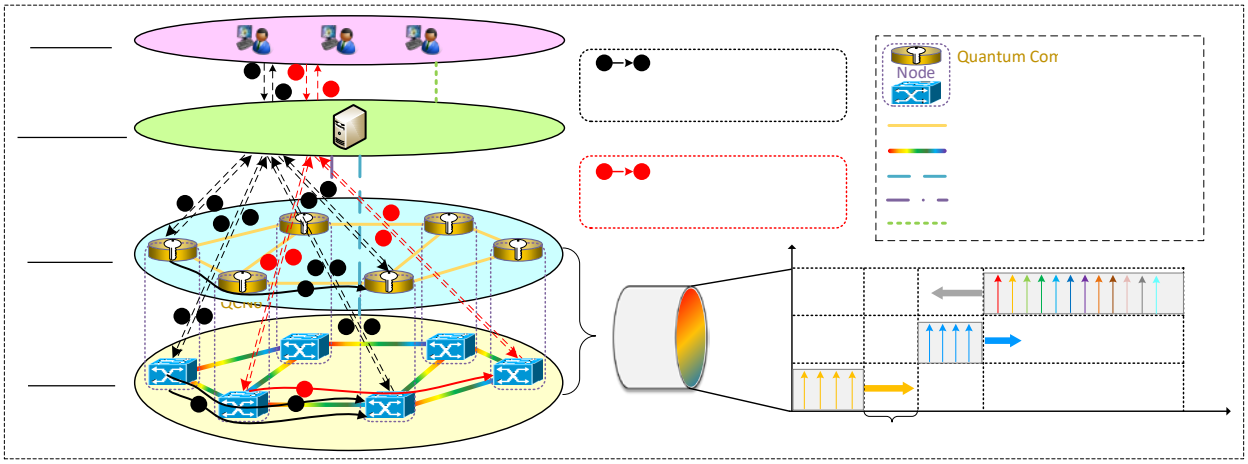

Figure 2. *QKD-enabled optical network architecture.*

2.3 Problem statement

As shown in Fig. 2, connection requests with different security demands require the allocation of three types of channels. Since wavelength resources in an optical fiber are limited and most of the wavelengths should be used to support large confidential data transmission, we investigate a solution in which QSCh and PICh share wavelength capacity using optical time-division multiplexing (OTDM). To realize secure key synchronization and reduce the negative impact of physical-layer impairments, QSCh and PICh should occupy separate wavelength channels with a large guard band (e.g., 200 GHz) between them as illustrated in Fig. 2. The wavelengths for QSCh and PICh can be divided into multiple time slots, and each time slot can be used to build a QSCh or a PICh. Hence, the time-slot assignment problem must be addressed in a QKD-enabled optical network.

The routing, wavelength, and time-slot assignment problem has been investigated in OTDM networks [13]. However, different from traditional RWTA, the new feature in a QKD-enabled optical network is that the secure key for a TDCh should be updated periodically according to specific security-level requirements (if we adopt, e.g., the AES encryption algorithm [14]). Specifically, the secure keys must be frequently updated to prevent the encrypted data being cracked by eavesdroppers. Hence, time slots in QSCh and PICh should be re-allocated periodically to update the secure key for the connection request with a specific security level. The key-updating period is the period after which the secure key has to be changed between two end-points. The security level increases while shortening the key-updating period. As another difference with traditional resource-allocation problems in optical networks [15], resource allocation for QSCh, PICh, and TDCh in a QKD-enabled optical network must be performed together (i.e., it must be decided which and how many wavelengths to assign for QSCh, PICh, and TDCh), which is another new topic in this area.

3. Security Levels Based on Different Key-Updating Periods

The security level of a connection depends on the length of the key-updating period (denoted as *T* hereafter). The security level becomes higher when *T* becomes smaller, because the secure key is changed more frequently, which will increase the difficulty

of acquiring the secure key for the eavesdropper. Moreover, security level increases when more diverse values of *T* are employed, because the required time for an eavesdropper to know the value of *T* is increased. In this article, two different schemes are proposed to set the security level of a connection request based on the configuration of key-updating periods, as described below.

3.1 Scheme 1: Security level configuration with fixed *T*

In the first scheme, the key-updating period *T* is configured with a fixed value for each connection request, but connection requests with different security levels have different values of *T*. We can identify two subcases of this scheme (Fig. 3(a)). In case 1, *T* is the same for all the wavelengths reserved for QSCh (and PICh). In case 2, *T* has the same value over the same wavelength reserved for QSCh (and PICh), but it changes over different wavelengths. For example, if there are four wavelengths reserved for QSCh (and PICh), only one value of *T* is possible in case 1, whereas four values of *T* can be used in case 2.

3.2 Scheme 2: Security level configuration with flexible *T*

To improve the security level of connection requests, key-updating period *T* can be flexibly configured according to some statistical distributions. This can be considered as another dimension of security improvement. Since *T* changes dynamically, it will be more difficult for the eavesdropper to know the value of *T* due to the increased time complexity; and this, in turn, enhances network security. As an example, we consider the case where the key-updating period *T* can be configured according to a Gaussian distribution. Note that the information on *T* value is exchanged between two end-points through the PICh.

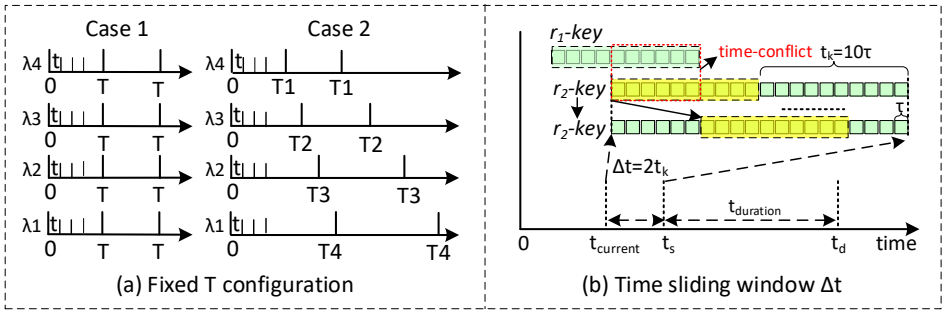

Figure 3. *Different security levels with different key-updating periods.*

4. Routing, Wavelength and Time-Slot Assignment (RWTA) in QKD-Enabled Optical Networks

To effectively operate a QKD-enabled optical network, we propose a novel RWTA algorithm to allocate resources for the three types of channels (TDCh, QSCh, and PICh), while considering the two schemes to set the security levels proposed in Section 3. As described in Section 2, the length of a time slot is set as the maximum key-synchronization time in the network (i.e., the synchronization time needed over the longest path and with the lowest qubit transmission rate). Hence, we can assume that a 256-bit key can be synchronized between any pair of end-points within the assumed time-slot duration. Note that a time conflict may occur in the procedure of RWTA when the two connection requests arrive dynamically and require time slots on the same wavelength for key synchronization. For example, in Fig. 3(b), connection request 1 (r_1) arrives first, and a time slot (r_1-*key*) is allocated to r_1 for key synchronization. After a while, and before the key synchronization for r_1 is finalized, connection request 2 (r_2) arrives. If a time slot (r_2-*key*) is allocated to r_2 for key synchronization immediately, a time conflict will occur between r_1-*key* and r_2-*key*. A scheduling solution must be adopted to avoid the time conflict of key synchronization. The concept of time-sliding window (TSW) is introduced in RWTA algorithm to address this problem.

4.1 Time-sliding window (TSW)

In a QKD-enabled optical network, a connection request is denoted as $r(s, d, t_s, t_d, \Delta t)$, where *s* and *d* are source and destination nodes; t_s and t_d are start time and end time of data transfer; Δt is the time width of TSW, which is composed of several time slots. τ is the smallest time granularity of the TSW. Additionally, t_k is defined as the key-synchronization time (i.e., a time slot). As shown in Fig. 3(b), $t_{current}$ is the current time, i.e., time when the connection request arrives at the SDN controller, and t_s is time when the data transfer starts. Note that t_s is equal to $t_{current}+\Delta t$, which means that the end-points have to wait for Δt to receive the secure key and then encrypt the messages before data transfer.

When the SDN controller receives $r(s, d, t_s, t_d, \Delta t)$, TDCh for *r* will be calculated and reserved; then the lightpath will be built at t_s after receiving the secure key. Specifically, Δt can be set as 0, t_k, or any value larger than t_k. When Δt is set as 0, it denotes that the connection request *r* has no security requirement, because there is no time for key synchronization. When Δt is set as t_k, the connection request has a security requirement, and the related QSCh and PICh must be built immediately upon receiving the connection request. When Δt is larger than t_k, the related QSCh and PICh can start to be built anytime within the interval $[0, \Delta t - t_k]$. Here, we set $\Delta t = 2t_k$ as an example in Fig. 3(b), in which QSCh and PICh can be built at any time within $[0, t_k]$ with TSW. In Fig. 3(b), we set $t_k = 10\tau$. Considering the time interval $[0, 5\tau]$ has been occupied by the r_1-*key*, the connection request *r* can find a time slot of size t_k to build QSCh and PICh within $[6\tau, 10\tau]$. The parameter, Δt, can be used to reduce the occurrence probability of time conflicts for secure key synchronization.

4.2 RWTA algorithm with TSW

A RWTA algorithm is proposed with TSW for a QKD-enabled optical network, which consists of three steps as shown in Fig. 4. In step 1, TDCh is allocated on the physical topology according to K-shortest path (KSP) routing algorithm and First Fit (FF) wavelength-allocation algorithm. $W(P)$ in this step is defined as the set of available wavelength resources on the selected route of a connection. Resource allocation for PICh is same as QSCh because they all occupy a time slot for secure key synchronization as described in Section 2. Note that each connection request allocates an entire wavelength for TDCh, and a time slot for QSCh (PICh). In step 2, Dijkstra algorithm is used to compute and select a specific route of QSCh (and PICh) on the physical topology, and FF algorithm is used to allocate time slots for QSChs (and PICHs). Different from step 1, time slots are allocated for each connection request with secure key demand in step 2, and different values of TSW can be used for different connection requests. Step 3 is used for key updating for the connection request. Dijkstra algorithm is also used for routing computation. In steps 2 and 3, $WT(P)$ is defined as available time-slot set on the wavelengths reserved for QSCh (and PICh) through the computed route. In this algorithm, Δt and T can be set as different values to evaluate related performance.

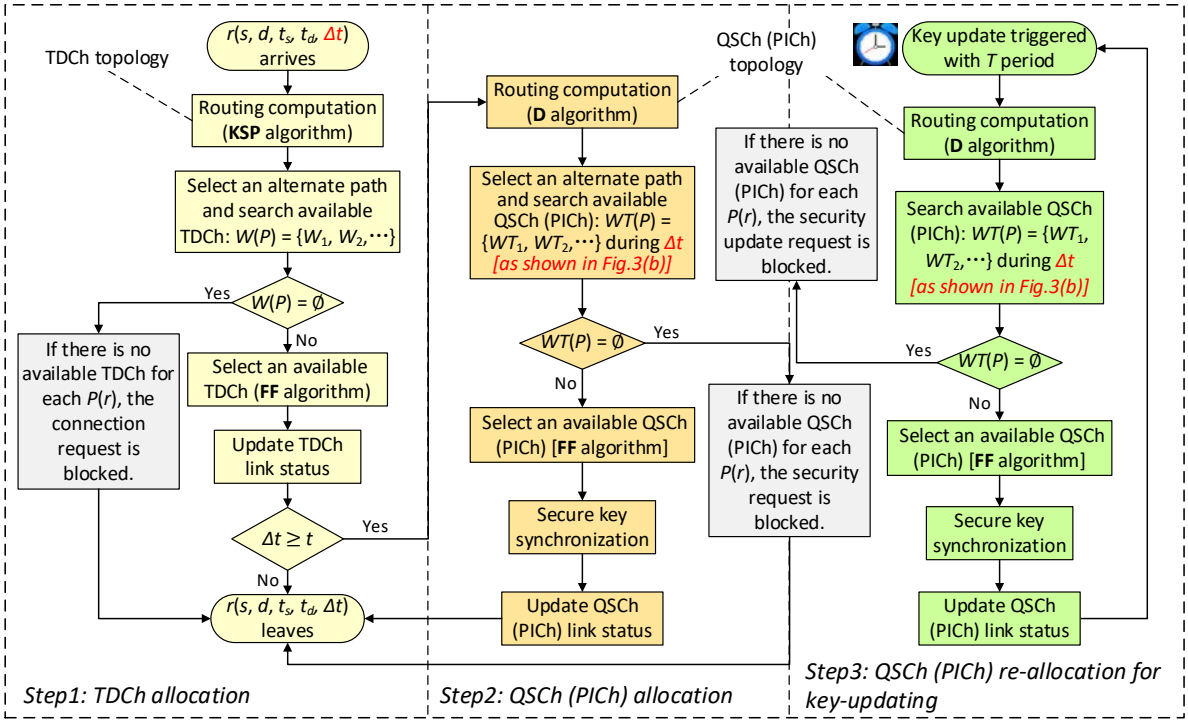

Figure 4. *RWTA algorithm with TSW for a QKD-enabled optical network.*

5. Simulation Results and Discussion

To verify the performance of RWTA algorithm for a QKD-enabled optical network, we perform discrete-event simulation of QKD-enabled optical networks (considered as a loss system) where connection requests are dynamically generated according to a Poisson distribution and are randomly distributed among all node pairs. Optical circuit switching (OCS) with wavelength continuity is considered. The parameters for simulation are shown in Fig. 5(a). In the following, the impacts on blocking probability of different key-updating periods (T), different TSWs, and different number of wavelengths allocated to the three types of channels are simulatively evaluated and discussed.

5.1 Security scheme 1 with different fixed T

Simulations of security scheme 1 with different values of fixed T per wavelength values are conducted first. Four wavelengths are reserved for QSCh and PICh. Blocking probability of QSCh (and PICh) connection (Fig. 5b) considers initial-key requests and key-update requests together, i.e., QSCh (and PICh) connection is blocked if there is not enough capacity in the wavelength to accommodate an initial-key request or a key-update request. Hence, blocking probability of QSCh (and PICh) is defined as the ratio of connections that failed to obtain the keys (including initial keys and all the update keys within holding time) to the total number of connection requests. Resource utilization of QSCh (and PICh) (Fig. 5c) represents the average utilization of the four wavelengths reserved for QSCh (and PICh). The probability of key-update failure (Figs. 5d and 5e) is defined as the ratio of connection requests with key-update failure to the total number of connection requests.

As shown in Fig. 5(b), blocking probability of QSCh (and PICh) increases for increasing traffic load, while it decreases for increasing value of the key-updating period T (as, for larger T, the number of key-update requests decreases). Accordingly, resource utilization of QSCh (and PICh) decreases when the key-updating period increases (Fig. 5(c)). As illustrated in Figs. 5(d)

and 5(e), the probability of key-update failure (e.g., partial key-update failure and all key-update failure within the holding time) of all the connections also increases for increasing traffic load (or for decreasing *T*), which mainly results from the increase of the number of key-update requests. Here, key-update failure means that QSCh (PICh) is blocked. Simulation results also indicate a trade-off between the QSCh (and PICh) blocking probability and the security level. Note, in fact, that the security level is higher when *T* is smaller (as the key is updated more frequently), but smaller values of T induce higher QSCh (and PICh) blocking probability.

Network topology	NSFNET
Number of nodes	14
Number of bi-directional links	21
Number of wavelengths on each link	40
Number of wavelengths as guard band	4
Number of time slots on each QSCh (and PICh)	T/t_k
The length of a key for each key-request (or key-update)	256 bits
Number of connection requests	10000
Key-updating period	T
Key synchronization time (i.e., one time slot)	t_k
Time-sliding window	TSW

(a) Simulation parameters

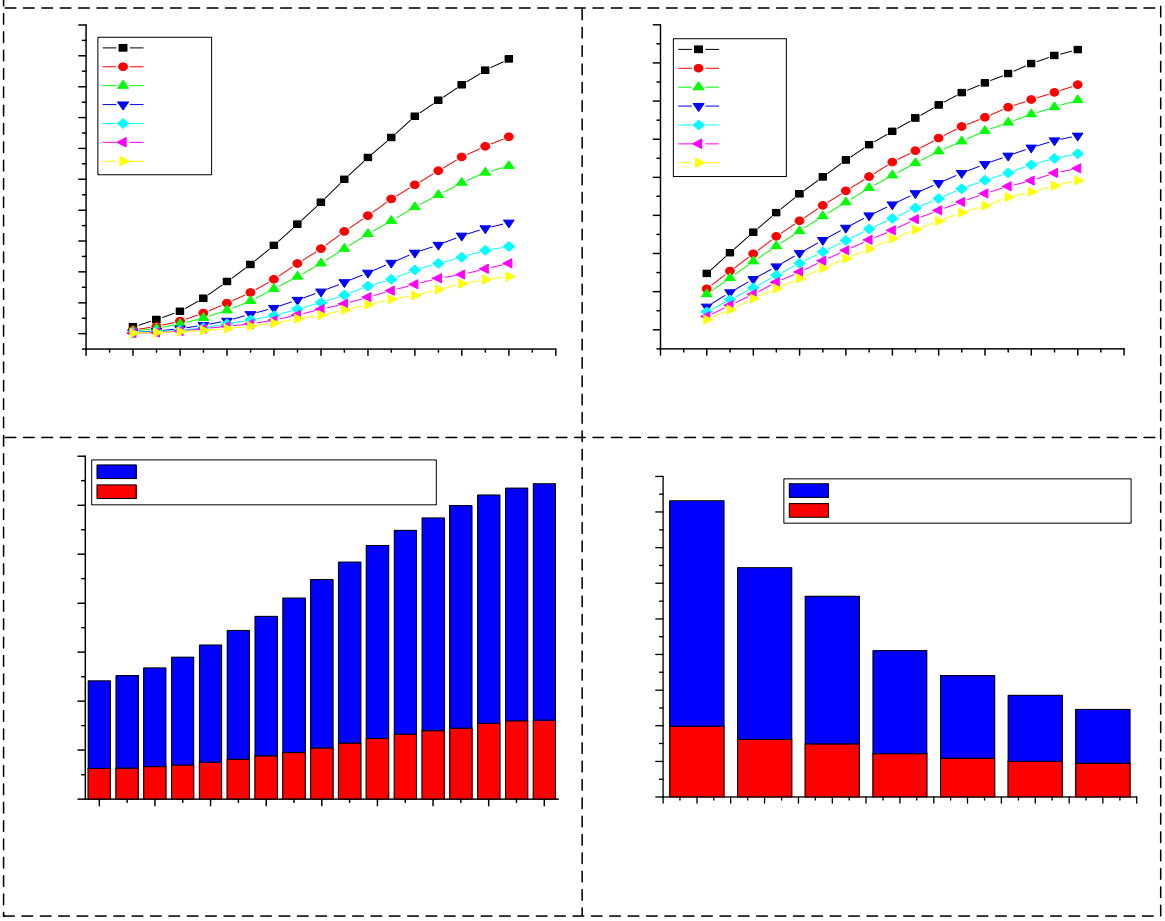

Figure 5. *(a) Simulation parameters; (b-e) performance verification with different T and traffic load.*

5.2 Security scheme 2 with different flexible *T*

Based on the description in Section 3, to improve the security performance of connection requests, security scheme 2 with different flexible T can be used, where key-updating period T is randomly generated over a certain range. The average value of T is set as $10t_k$. The security level will become higher when the range of T is expanded, because the value of T becomes more difficult to be known by the eavesdropper. On the other hand, as shown in Fig. 6(a), blocking probability of QSCh (and PICh) increases when the range of T is expanded because the types of security level are increased, which illustrates that security of connection requests can be improved only at cost of increasing blocking probability.

5.3 Different TSWs

In Section 4, we introduced the parameter "TSW" to reduce the occurrence probability of time conflicts during key synchronization among different connection requests. As the simulation results show in Fig. 6(b), different value of TSWs are adopted among [t_k, $1.5t_k$, $2t_k$, $3t_k$, $4t_k$]. Blocking probability of QSCh (and PICh) can be reduced by increasing the value of TSW, but there is no additional gain while increasing the value of TSW beyond $3t_k$. The reason is that wider TSW provides more opportunities for the time-slot allocation of connection requests. Thus, we conclude that the optimal performance of blocking probability can be achieved with a limited TSW without sacrificing many time slots.

5.4 Different number of wavelengths for the three types of channels

Now, three simulation scenarios are considered in which 2, 4, and 6 wavelengths are allocated for QSCh and for PICh. Therefore, excluding the four wavelength channels reserved as guard band for QSCh and PICh, 32, 28, and 24 wavelengths allocated remain for TDCh. The key-updating period is fixed as $10t_k$, and TSW is configured as $3t_k$. Blocking probabilities of TDCh and QSCh (and PICh) are shown in Figs. 6(c) and 6(d). Blocking probability of QSCh (and PICh) decreases and blocking probability of TDCh increases with the number of QSChs (and PICHs) increasing, which results from the reduction of allocated wavelength resources. More studies are needed to strike the right balance in wavelength allocation between QSCh (and PICh) and TDCh in an optical network secured by QKD.

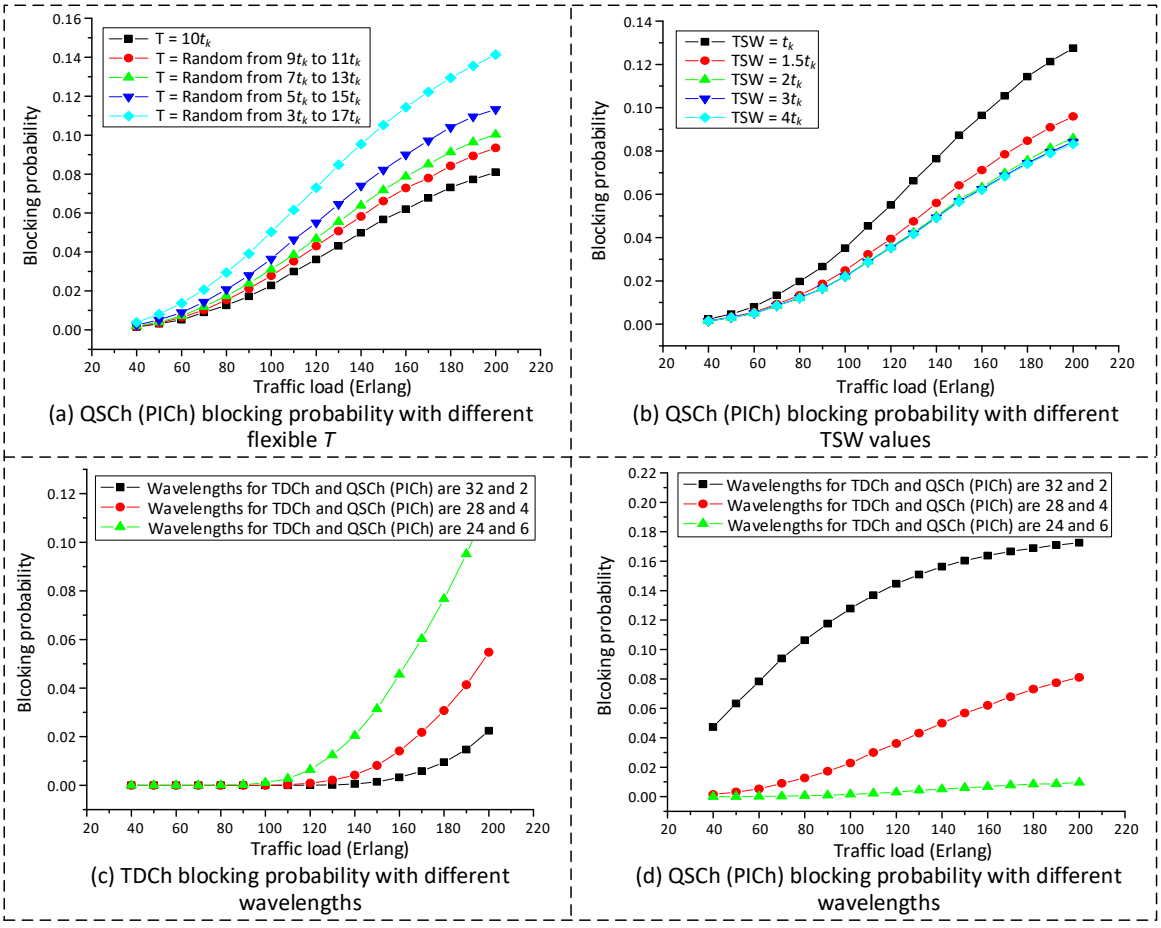

Figure 6. *Blocking probability with different configuration methods.*

6. Open Issues

Most current research focuses on how to improve the bit rate and transmission distance of qubits using existing optical fiber channel. However, there are several research issues on the networking aspect of a QKD-enabled optical network to be addressed if we want to effectively provision the three types of channels QSCh, PICh, and TDCh. Some open issues are stated below.

6.1 Trusted repeater node placement

Transmission distance for qubits is a very important problem in a QKD-enabled optical network, which can be solved by trusted repeater node (TRN) placement. How to place the TRN in a QKD-enabled optical network is of great importance due to the high cost and deployment difficulty. Some placement methods can be studied for TRN to achieve different optimization objectives, such as cost, location, and security performance.

6.2 Resiliency in a QKD-enabled optical network

QKD can provide secure keys for end-to-end lightpaths and improve the security of an optical network. However, how to guarantee survivability in a QKD-enabled optical network is a new topic. QSCh and PICh should be protected simultaneously in a QKD-enabled optical network. Especially due to the utilization of key-updating period with different time slots, protection action will occur at sub-wavelength level. Synchronization might also represent a difficult problem for QSCh and PICh.

6.3 How to make full use of bandwidth resources on QSCh and PICh

In a QKD-enabled optical network, QSCh and PICh are used for key synchronization. In this article, t_k is assumed to be fixed as the key-synchronization time under the worst-case scenario in a QKD-enabled optical network. In reality, the latency for each key synchronization may vary because it is related to key size and route selection. Also, physical-layer effects (e.g., loss and scattering) may impact the key-synchronization time and key rate. Then, how to make full use of time-slot resources on QSCh and PICh is another open issue.

7. Conclusion

A QKD-enabled optical network architecture is described, in which control plane is realized by using SDN, and QKD plane is designed to provide secure keys for end-to-end lightpaths. Three types of channels (TDCh, QSCh, and PICh) can be constructed by an SDN controller over different wavelengths located in fiber C-band. For the first time, we investigate the resource-allocation problem in an optical network secured by QKD. A RWTA algorithm is designed for the resource allocation of the three types of channels. Different security levels can be considered in the RWTA algorithm, by tuning the time period *T* of key updating for each connection request. Simulation results show that the key-updating period has an important impact on the performance of blocking probability of QSCh (and PICh), which will become higher when *T* is shorter, but the security performance is better. While adopting security level scheme 2, the security of connection requests can be improved by extending the range of *T* selection at the cost of increasing blocking probability. To avoid time conflict in key synchronization, TSW is introduced into RWTA algorithm. Finally, some open issues in QKD-enabled optical networks are discussed, such as TRN placement, resilience in a QKD-enabled optical network, and how to make full use of bandwidth resources on QSCh and PICh.

Acknowledgment

This work was supported by China's NSFC Grant No. 61571058 and BUPT Excellent Ph.D. Students Foundation (CX2016310). This work was also supported by NSF Grant No. CNS-1217978.

References

[1] P. J. Winzer, "Scaling Optical Fiber Networks: Challenges and Solutions," *Optics and Photonics News*, vol. 26, no. 3, pp. 28–35, Mar. 2015.
[2] J. Zhu *et al.*, "Attack-Aware Service Provisioning to Enhance Physical-Layer Security in Multi-Domain EONs," *J. Lightwave Technol.*, vol. 34, no. 11, pp. 2645–2655, June 2016.
[3] M. P. Fok *et al.*, "Optical Layer Security in Fiber-Optic Networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 725–736, Sept. 2011.
[4] P. Jouguet *et al.*, "Field Test of Classical Symmetric Encryption with Continuous Variables Quantum Key Distribution," *Optics Express*, vol. 20, no. 13, pp. 14030–14041, June 2012.
[5] S. Debnath *et al.*, "Demonstration of a Small Programmable Quantum Computer with Atomic Qubits," *Nature*, vol. 536, pp. 63–66, Aug. 2016.
[6] H.-K. Lo *et al.*, "Quantum Cryptography," *Encyclopedia of Complexity and Systems Science*, vol. 8, pp. 7265–7289, Springer New York, 2009.
[7] A. V. Gleim *et al.*, "Secure Polarization-Independent Subcarrier Quantum Key Distribution in Optical Fiber Channel Using BB84 Protocol with a Strong Reference," *Optics Express*, vol. 24, no. 3, pp. 2619–2633, Feb. 2016.
[8] H.-K. Lo *et al.*, "Secure Quantum Key Distribution," *Nature Photonics*, vol. 8, pp. 595–604, July 2014.
[9] L. J. Wang *et al.*, "Experimental Multiplexing of Quantum Key Distribution with Classical Optical Communication," *Applied Physics Letters,* vol. 106, no. 8, pp. 081108.1–4, Feb. 2015.
[10] S. Bahrani *et al.*, "Optimal Wavelength Allocation in Hybrid Quantum-Classical Networks," *24th European Signal Processing Conference (EUSIPCO)*, Budapest, Hungary, Aug.-Sept. 2016.
[11] N. A. Peters *et al.*, "Dense Wavelength Multiplexing of 1550 nm QKD with Strong Classical Channels in Reconfigurable Networking Environments," *New Journal of Physics*, vol. 11, no. 4, pp. 045012.1–17, Apr. 2009.
[12] M. Peev *et al.*, "The SECOQC Quantum Key Distribution Network in Vienna," *New Journal of Physics*, vol. 11, no. 7, pp. 075001.1–37, July 2009.
[13] B. Wen *et al.*, "Routing, Wavelength and Time-Slot Assignment in Time Division Multiplexed Wavelength-Routed Optical WDM Networks," *IEEE INFOCOM 2002,* vol. 3, New York, USA, pp. 1442–1450, June 2002.

[14] M. Taha *et al.*, "Key-Updating for Leakage Resiliency with Application to AES Modes of Operation," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 3, pp. 519–528, Mar. 2015.
[15] Z. Zhu *et al.*, "Dynamic Service Provisioning in Elastic Optical Networks With Hybrid Single-/Multi-Path Routing," *J. Lightwave Technol.*, vol. 31, no. 1, pp. 15–22, Jan. 2013.

Author biography.

Yongli Zhao is currently an associate professor at Beijing University of Posts and Telecommunications (BUPT). He received Ph.D. degree from BUPT in 2010. During Jan. 2016 to Jan. 2017, he was a visiting associate professor at UC Davis. He has published more than 300 international journal and conference papers. Since 2015, he became a senior member of IEEE. His research focuses on software-defined optical networking, elastic optical networks, and optical network security. Email: yonglizhao@bupt.edu.cn

Yuan Cao received his B.S. degree in optoelectronic information engineering from the Nanjing University of Posts and Telecommunications, Jiangsu, China, in 2016. He is currently pursuing his Ph.D. degree in information and communication engineering at the Beijing University of Posts and Telecommunications, Beijing, China. His research interests include software-defined optical networking, elastic optical networks, quantum key distribution, and optical network security.

Wei Wang received his B.S. degree in communication engineering from Beijing University of Posts and Telecommunications (BUPT), in 2013. He is currently working toward the Ph.D. degree in information and communications engineering, at BUPT. He was a visiting research scholar at University of California, Davis, from October 2016 to October 2017. His research interests include software-defined networking, network function virtualization, and mobile edge computing.

Hua Wang received her B.S. degree in electronic information and science engineering from Xiangtan University (XTU), in 2016. She is currently pursuing the Ph.D. degree in information and communication engineering at Beijing University of Posts and Telecommunications, Beijing, China. Her research interest includes software-defined optical networks, quantum key distribution, and optical network security.

Xiaosong Yu received his Ph.D. degree from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2015, and was a visiting scholar in University of California, Davis during Sep. 2013 to Sep. 2014. Now he is an assistant professor of institute of information photonics and optical Communications (IPOC) in BUPT. Up to now, he has co-authored more than 50 journal and conference papers. His interested research focuses on SDM-EONs, SDON, and optical network security.

Jie Zhang is currently a professor and the dean of Information Photonics and Optical Communications Institute at Beijing University of Posts and Telecommunications (BUPT), China. He received Ph.D. in electromagnetic field and microwave technology from BUPT. He has published more than 300 technical papers, authored 8 books, and submitted 17 ITU-T recommendation contributions and 6 IETF drafts. His research focuses on architecture, protocols, and standards for optical transport networks.

Massimo Tornatore is an associate professor at Politecnico di Milano, Italy, and an adjunct professor at the University of California, Davis. He co-authored more than 280 technical papers (with 11 best paper awards), and his research interests include optimization, performance evaluation, application of machine learning in telecom and cloud networks. He received a Ph.D. degree in 2006 from Politecnico di Milano.

Yu Wu received his B.E. degree in Information & Communication Engineering from Zhejiang University, China, in 2014. He is currently pursuing Ph.D. degree in Computer Science at University of California, Davis. His research interests include cloud and optical networks resource management, green energy communication, and 5G emerging technologies.

Biswanath Mukherjee is a Distinguished Professor at University of California, Davis. He received B.Tech. degree from Indian Institute of Technology, Kharagpur (1980) and Ph.D. from University of Washington, Seattle (1987). He was General Co-Chair of Optical Fiber Communications (OFC) Conference 2011, TPC Co-Chair of OFC '09, and Technical Program Chair of IEEE INFOCOM '96. He has served on eight journal editorial boards, most notably IEEE/ACM Transactions on Networking and IEEE Network..