Resource Allocation in Dynamic Optical Networks Secured by Quantum Key Distribution (QKD)

Yongli Zhao

BUPT & UC Davis
Tel : +86-10-61198108, Email: yonglizhao@bupt.edu.cn

UCDAVIS

Group Meeting, November 18, 2016

Outline

1. Background of optical layer security and QKD
2. QKD-enabled optical networks architecture
3. New issue in optical networks secured by QKD
4. Security level denoted with key-updating period
5. Routing, wavelength and time-slots assignment (RWTA) algorithm with time-sliding window (TSW)
6. Simulation results and analysis

Background of optical layer security and QKD

Optical communication networks have become the most important information infrastructure today. More than two billion kilometers of fibers have been deployed globally [1].

Fiber-optic transmission has been thought of as extremely secure for a long time, but some incidents have dispelled this myth over the past decade. It is reported that there were 16 known attacks on fiber-optic cables in the San Francisco area in 2015. So, security remains to be an important issue in the optical layer.

Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages [2].

[1] Peter J. Winzer, "Scaling Optical Fiber Networks: Challenges and Solutions," Optics and Photonics News, 26 (3), 28-35 (2015).
[2] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki, "Secure quantum key distribution," Nature Photonics, vol.8, July 2014, pp.595–604.

Basic Principle of QKD-BB84

BB84 uses two pairs of states, with each pair conjugate to the other pair, and the two states within a pair orthogonal to each other. Pairs of orthogonal states are referred to as a basis. The usual polarization state pairs used are either the rectilinear basis of vertical (0°) and horizontal (90°), the diagonal basis of 45° and 135° or the circular basis of left- and right-handedness. Any two of these bases are conjugate to each other, and so any two can be used in the protocol.

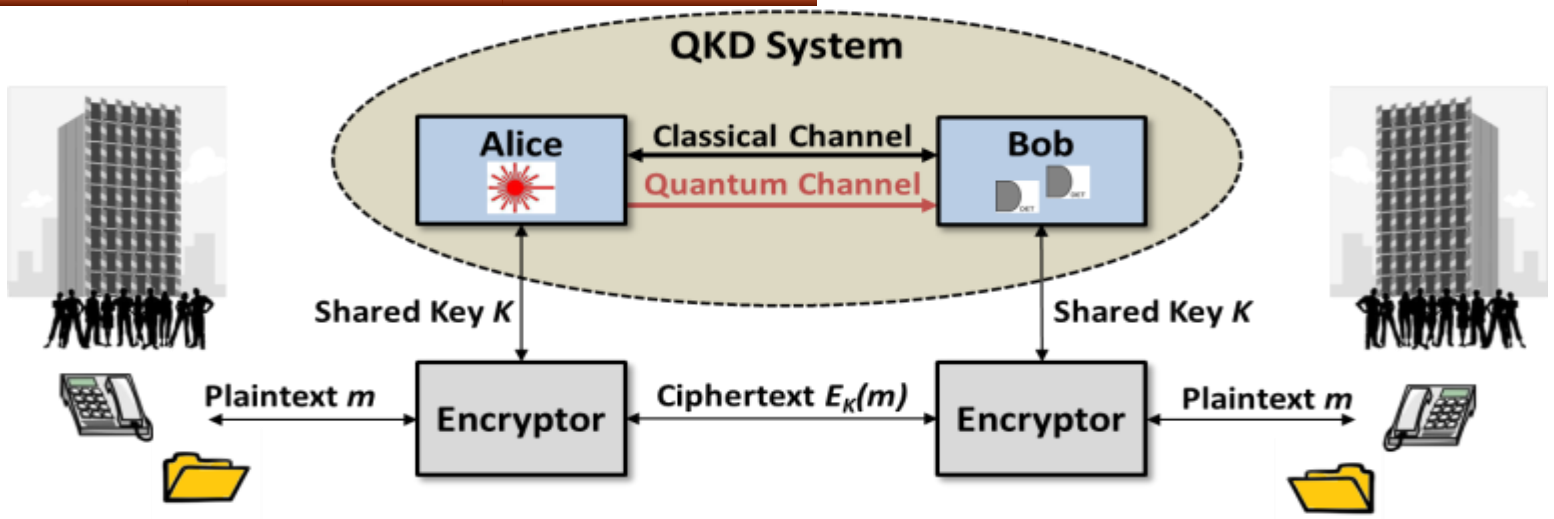
Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

Basis

Key

C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.

Basic Principle of QKD-BB84



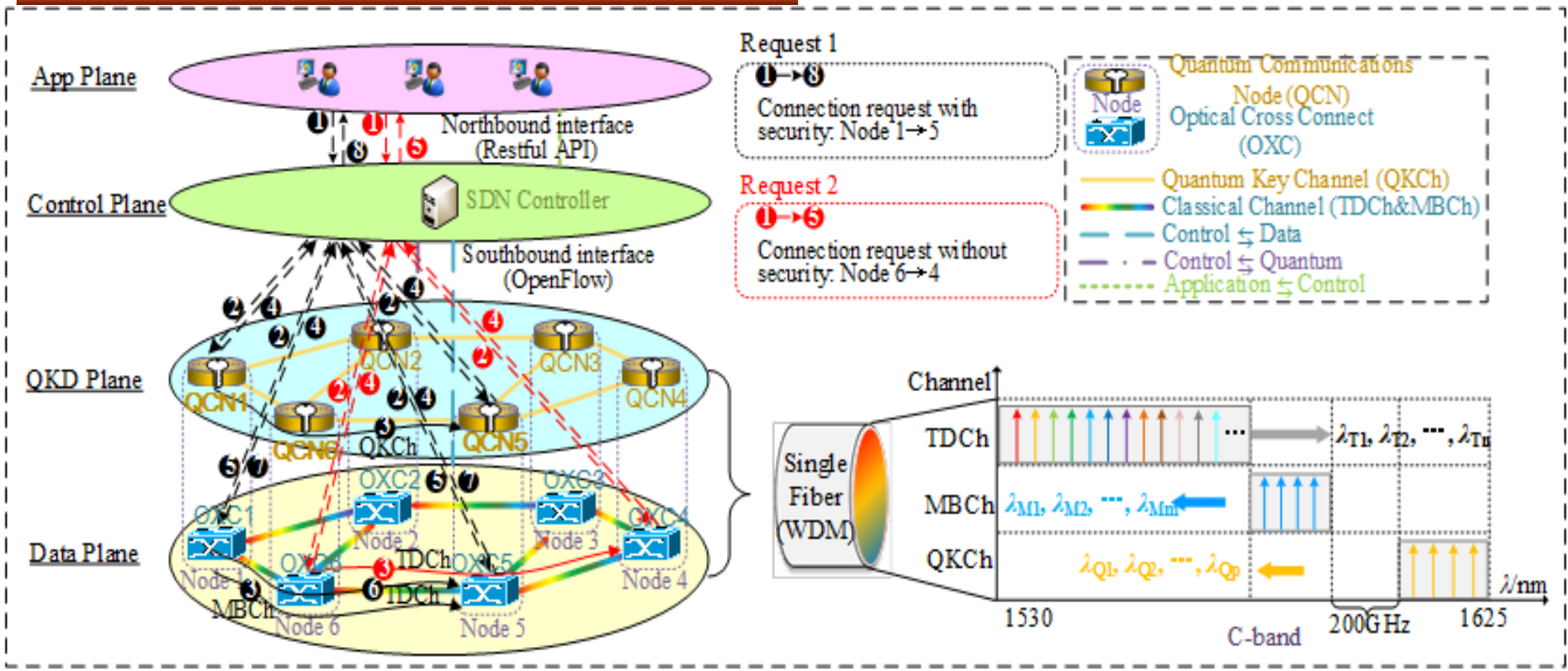
Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

Basis

Key

C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.

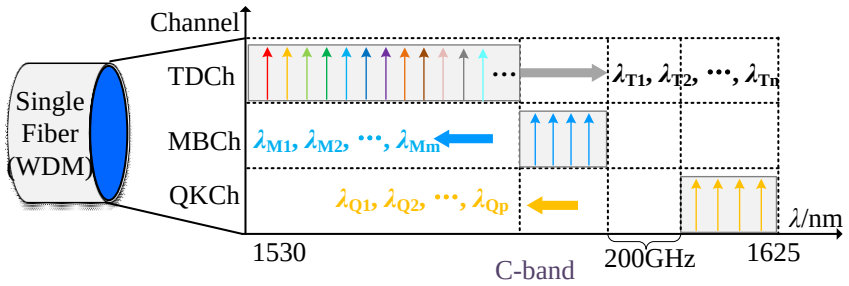
QKD-enabled optical networks architecture



The three types of channels are located at C-band to guarantee the optimal transmission performance. QKCh is located at rightmost C-band area to avoid Raman scattering effect, and 200GHz is reserved between MBCh and QKCh to achieve channel isolation and avoid four-wave mixing effect [3].

[3] N. A. Peters, P. Toliver, T. E. Chapuran, et al., "Dense Wavelength Multiplexing of 1550 nm QKD with Strong Classical Channels in Reconfigurable Networking Environments, " New Journal of Physics, vol. 11, April 2009.

New issue in optical networks secured by QKD



Since wavelength resources in optical fiber is limited, and quantum key (a series of bits) can be transmitted within a fixed time, OTDM technology can be adopted for QKCh and MBCh [4].

The wavelengths for QKCh and MBCh can be divided into multiple time-slots, and each time-slot is used to build a QKCh or MBCh. **Then, time-slot assignment becomes a new problem in QKD-enabled optical networks.**

Actually, routing, wavelength and time-slots assignment problem has been researched in OTDM networks.

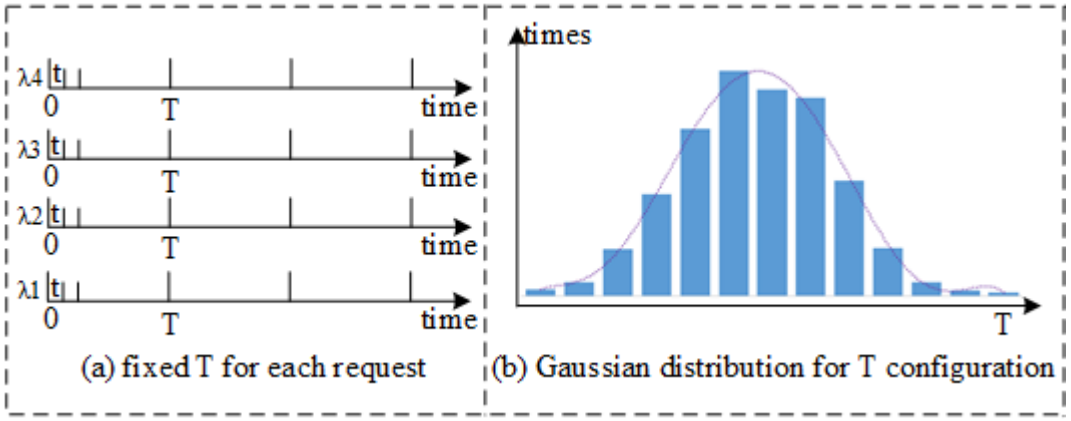
However, different from the traditional RWTA problem, the key should be updated at a period according to specific **security level** requirements [5], which means that a time-slot should be allocated for the service request every a period. Another point different from the traditional RWTA problem, the matching relationship between QKCh and TDCh should be considered in QKD-enabled optical networks.

[4] B. Wen and K. Sivalingam, "Routing, Wavelength and Time-Slot Assignment in Time Division Multiplexed Wavelength-Routed Optical WDM Networks," *in IEEE INFOCOM 2002,* vol. 3, New York, NY-USA, June 2002, pp. 1442–1450.

[5] Mostafa Taha, and Patrick Schaumont, "Key-updating for Leakage Resiliency with Application to AES Modes of Operation," *IEEE Transactions on Information Forensics and Security,* vol. 10, no.3, March 2015, pp.519-528.

Security level denoted with key updating period

To describe the security level clearly, a concept of quantum key-updating period is proposed, which is denoted as T. Different T values represents different security levels for service requests. The smaller T is, the higher security level will be. Meanwhile, the more types of T are, the higher security level will be.



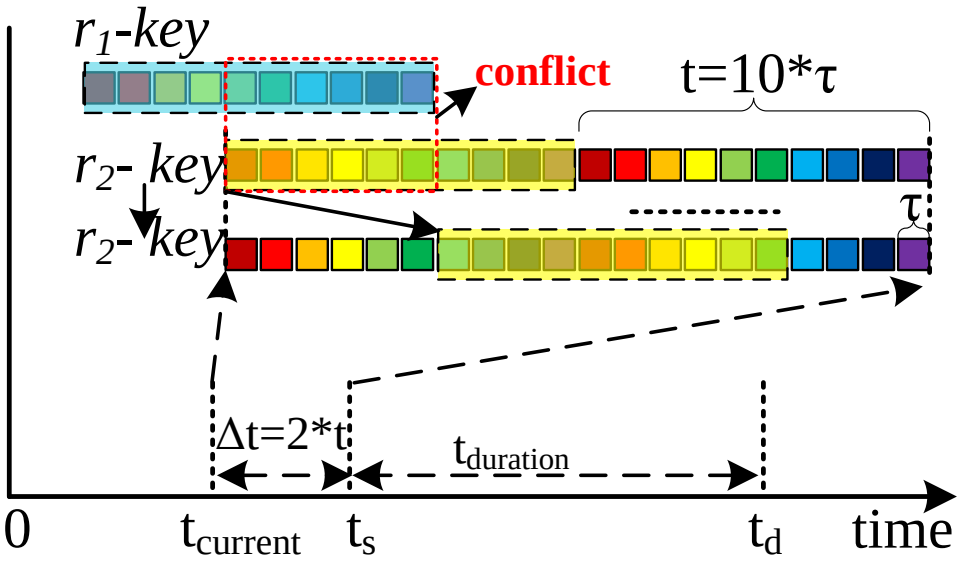
Scheme 1: security level denoted with fixed T

The key-updating period T (security level) for service requests is configured with fixed values. As shown in Fig. (a), all the service requests have the same fixed key-updating period on each wavelength.

Scheme 2: security level denoted with flexible T

The key-updating period T can be configured according to some distribution models, such as Gaussian distribution, Random distribution and Rayleigh distribution, which can be considered as another dimension of security improvement.

RWTA algorithm with TSW



time sliding window Δt

A conflict may occur when the service request arrives dynamically and may require time-slot on the same wavelength for quantum key transmission simultaneously. Especially for RWTA with key-updating period in dynamic network scenario, the QKCh connection requests are more likely to be blocked.

Request is denoted as $r\ (s, d, t_s, t_d, \Delta t)$, Δt is the TSW.

t is defined as key configuration time including key transmission, QKCh switching and setup.

$t_{current}$ is the current time, $t_s = t_{current} + \Delta t$.

Δt can be set as 0, t, or any value larger than t. When Δt is set as 0, it shows that r has no security requirement.

When Δt is set as t, the related QKCh must be built immediately upon receiving the connection request. When Δt is larger than t, the related QKCh can start being built within the $[0, \Delta t\text{-}t]$.

Here, we set $\Delta t = 2*t$ as an example. τ is the smallest time granularity of the TSW, which means that control plane can choose when to start building QKCh by setting the start time of the TSW within $[0, \Delta t\text{-}t]$ and sliding the window by integral multiples of τ to the right. We set $t = 10*\tau$ as an example, within Δt, there are ten possible positions for r to find a time-slot of size t to build the QKCh.

Thank you for your attention!

Yongli Zhao

BUPT & UC Davis
Tel : +86-10-61198108, Email: yonglizhao@bupt.edu.cn