Resource Map Construction in Security-hungry Optical Networks with Quantum Key Distribution

Yongli Zhao

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

UCDAVIS

Group Meeting, September 23, 2016

Outline

1. Basic Principle of QKD
2. Necessity of QKD Integrated with Optical Networks
3. QKD enabled Optical Networks with SDN
4. Resource Map Construction Problem in QKD enabled Optical Networks
5. Resource Map Design Algorithm in QKD enabled Optical Networks
6. Simulations to be done

Basic Principle of QKD

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.

An important and unique property of QKD is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies.

Quantum communication involves encoding information in quantum states, or qubits, as opposed to classical communication's use of bits. Usually, photons are used for these quantum states. QKD exploits certain properties of these quantum states to ensure its security, such as quantum indeterminacy and entanglement.

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.

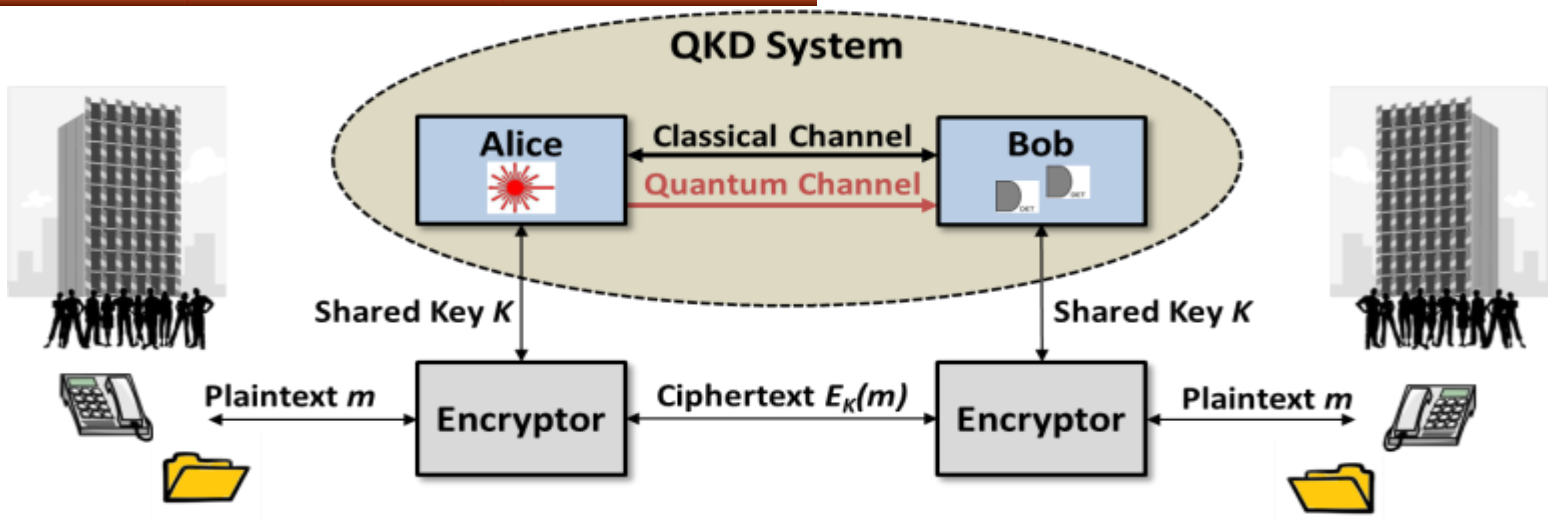
Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

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

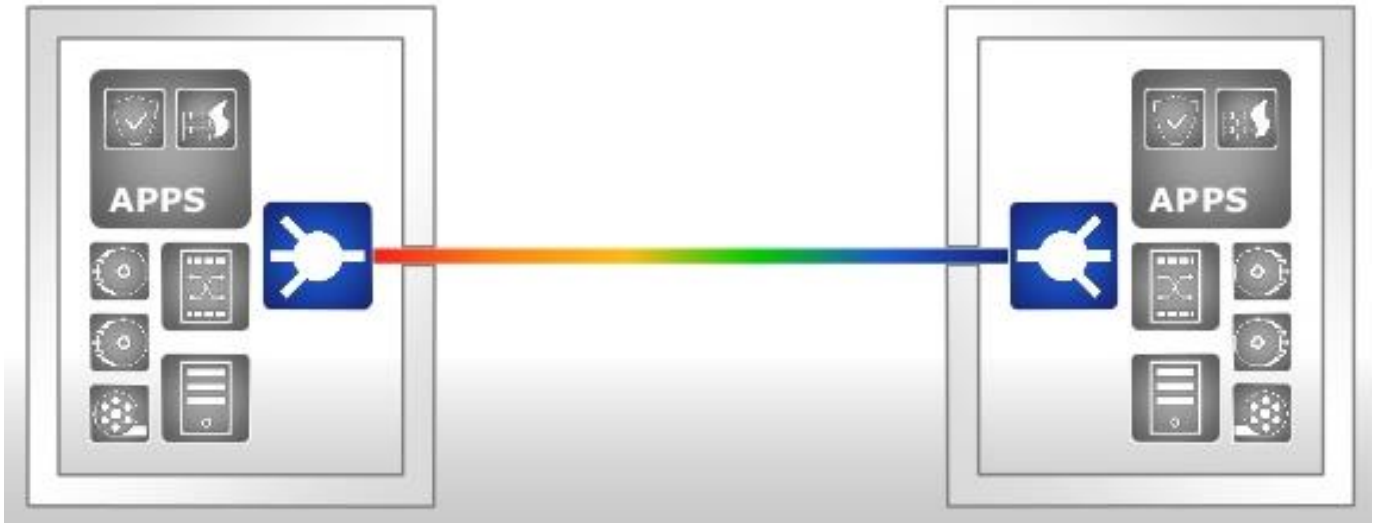
Key

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.

Necessity of QKD Integrated with Optical Networks

Optical communication networks have become the most important information infrastructure today. More than two billion kilometers of fibers have been deployed, and billions of mobile phone users are immediately converted to infrared photons. 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 in optical layer becomes an important issue.

Important → *Weak* → *Security* → *QKD*



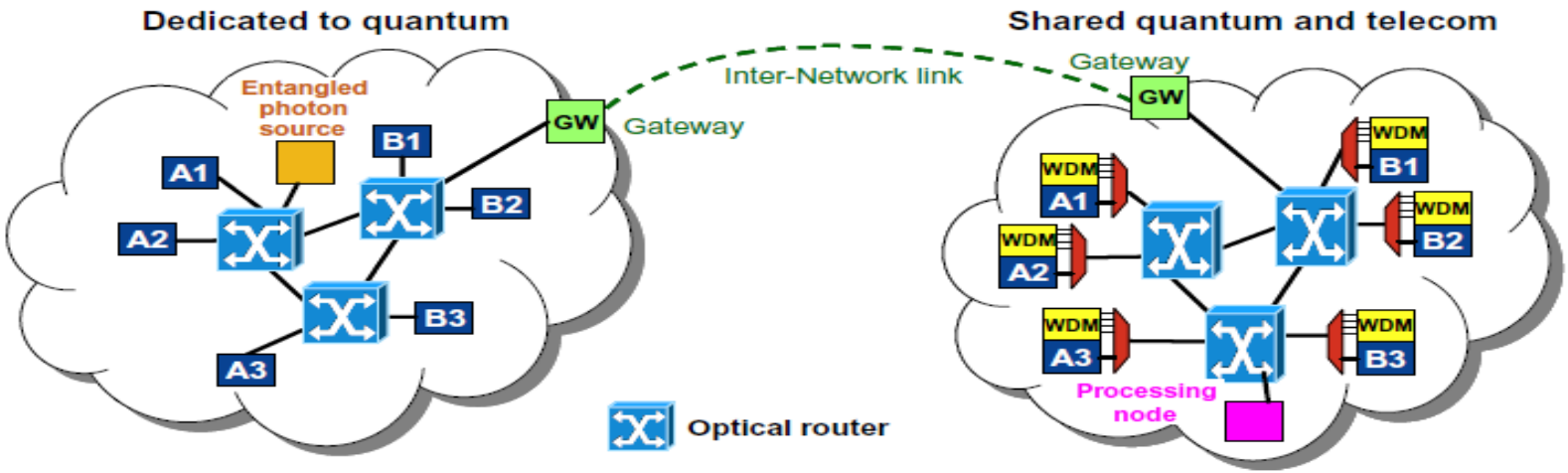
Peter J. Winzer, "Scaling Optical Fiber Networks: Challenges and Solutions," Optics and Photonics News, 26 (3), 28-35 (2015).

Necessity of QKD Integrated with Optical Networks

Optical fiber is the best carrier of quantum communications channel, although the transmission distance is limited by the loss in optical fibers to about 200 km. Achieving a final key generation rate of 1 Mb/s after 50-km transmission is still a challenge. (Trusted repeater node can be solution)

Since QKD is based on point-to-point transmission, it cannot be straightforwardly expanded for multiple-user key distribution.

Integration of QKD into existing optical communication networks has been considered as a solution for the issues mentioned above.



Cost-efficient solution

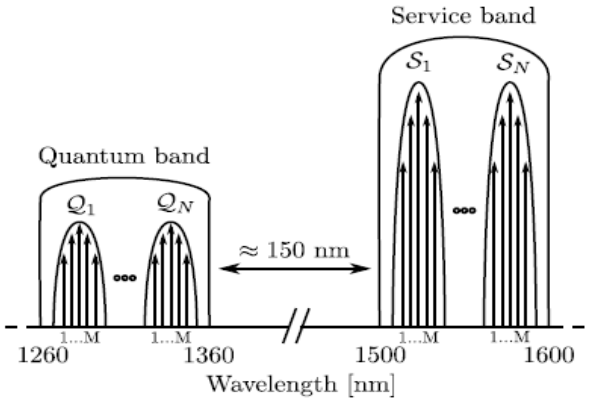
Necessity of QKD Integrated with Optical Networks

Some pioneering works have been done in this area [a].

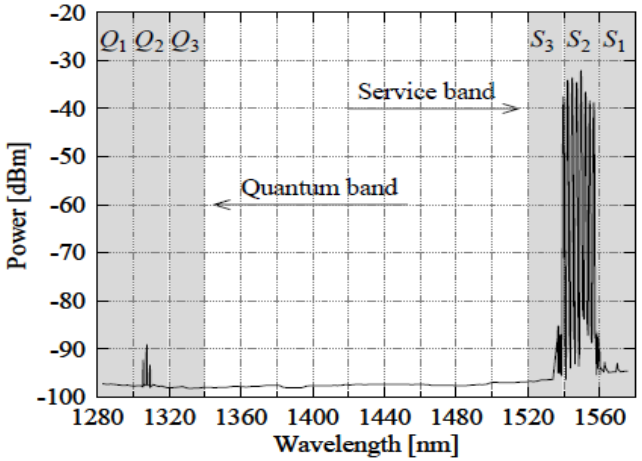
- ✓ QKD transmission over PON [18-20]
- ✓ Giga-bit transmission over a PON [21]
- ✓ Optical path switching in QKD transmission [22-25]
- ✓ Cotransmission of QKD signals with optical data [26-29]
- ✓ Key relay between trusted nodes [30, 31]
- ✓ Integrated networks have been demonstrated in DARPA Quantum network [23] and SECOQC QKD network [32]

QKD system shares WDM channels with data channels [b,c]

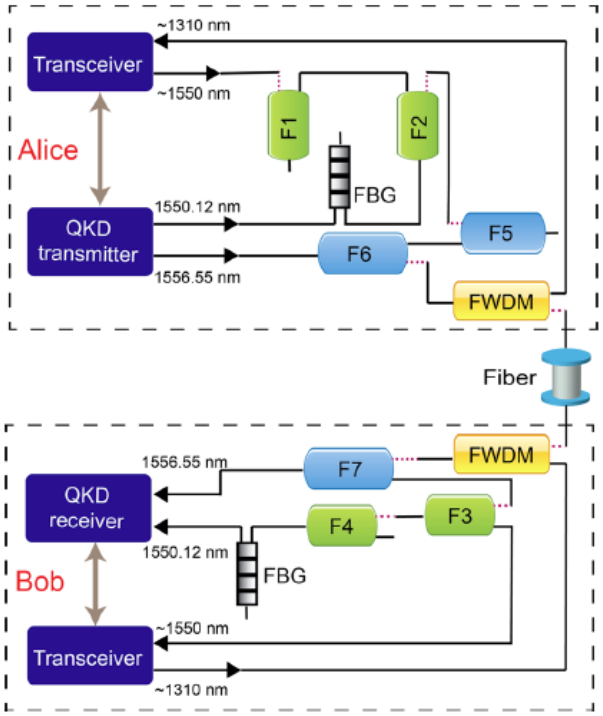
Conclusion:
Integration is feasible, quantum channel is located with O band, separated with classical channel located with C+L band.



(a)

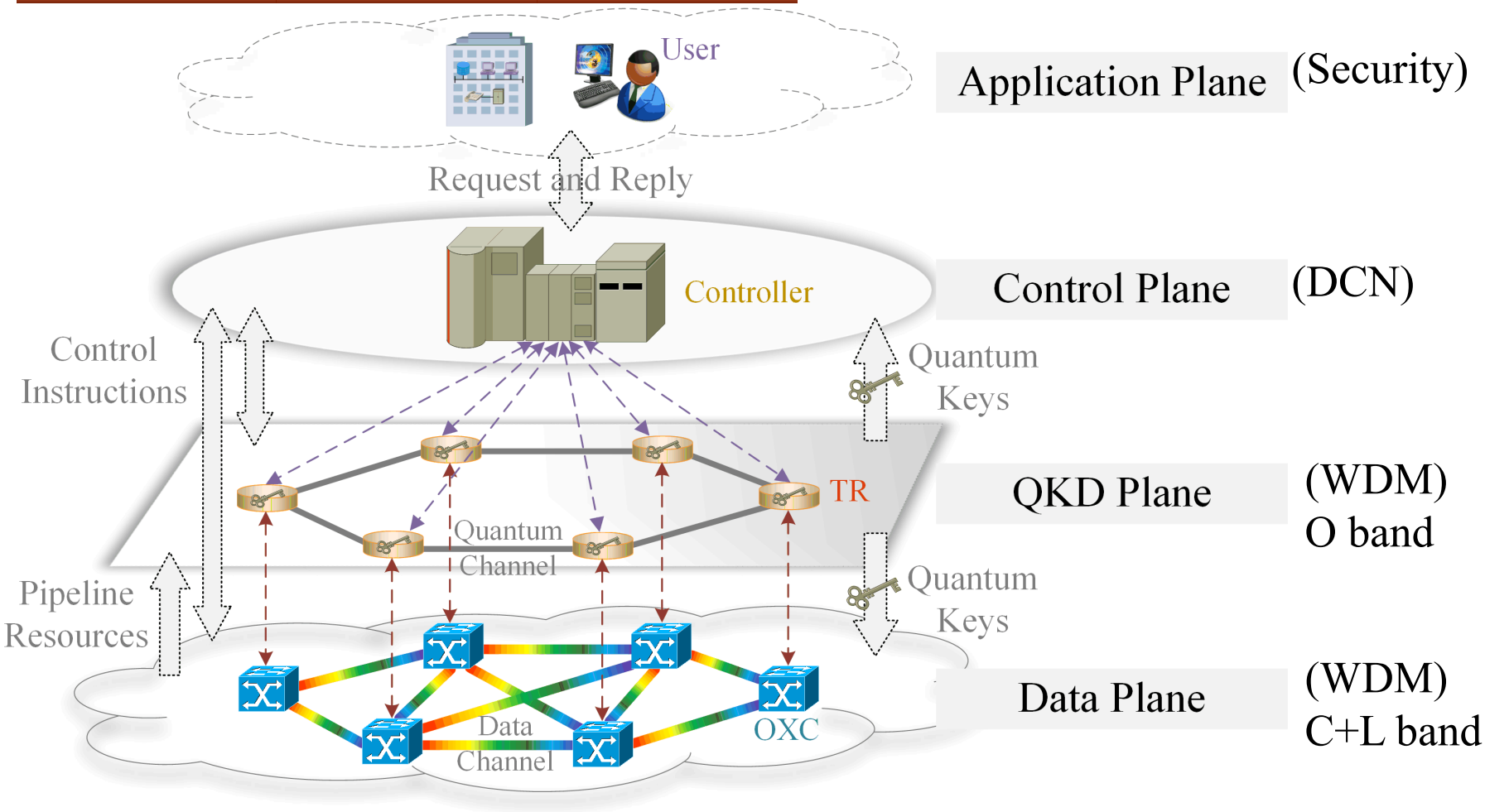


(b)



a. Wakako Maeda, Akihiro Tanaka, Seigo Takahashi, et al. Technologies for Quantum Key Distribution Networks Integrated With Optical Communication Networks, IEEE Journal of Selected Topic in Quantum Electronics, vol.15, no.6, Nov. 2009.
b. Ciurana,1 J. Mart´ınez-Mateo,1 M. Peev, et al. Quantum metropolitan optical network based on wavelength division multiplexing, vol.22, no.2, Jan. 2014.
c. Liu-Jun Wang, Luo-Kan Chen, Lei Ju, et al. Experimental multiplexing of quantum key distribution with classical optical communication, APL, 2015.

QKD enabled Optical Networks with SDN

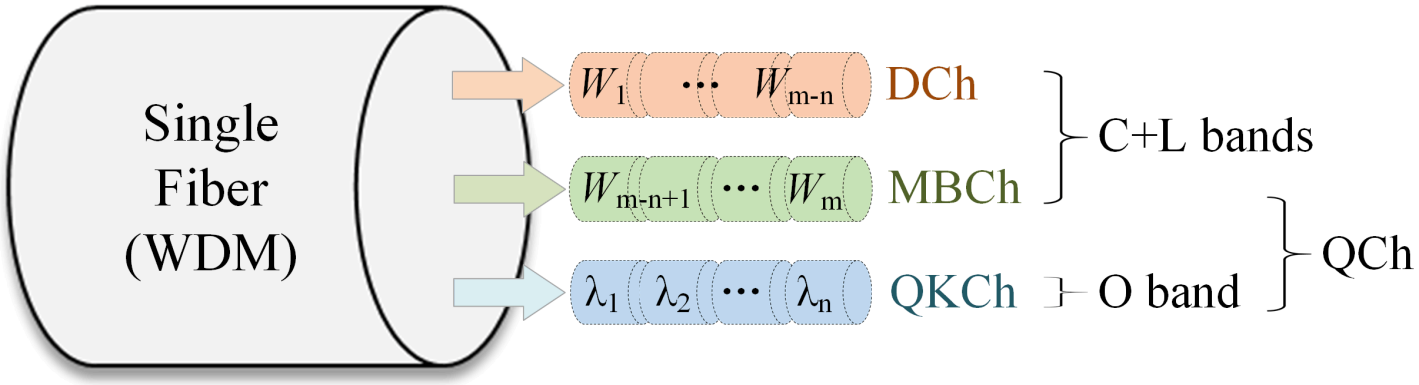


QKD plane and data plane share the wavelength resources in optical fiber to save cost and improve resource utilization. Then, how to allocate wavelength resources for three kind of channels and construct the resource map is a novel and important topic.

Resource Map Construction Problem in QKD-ON

Three kind of channels share the wavelength resources in the optical fiber, which are quantum key channel (QKCh), measuring basis channel (MBCh), and data channel (DCh).

Data Channel (DCh) often locate at C-band and L-band, then QKCh can chose O-band to achieve effective isolation, although a little more loss may be introduced. Besides, MBCh can be placed in C+L bands as the classical channels



QKCh: wavelengths at O band, W_O (assumed to be 4)

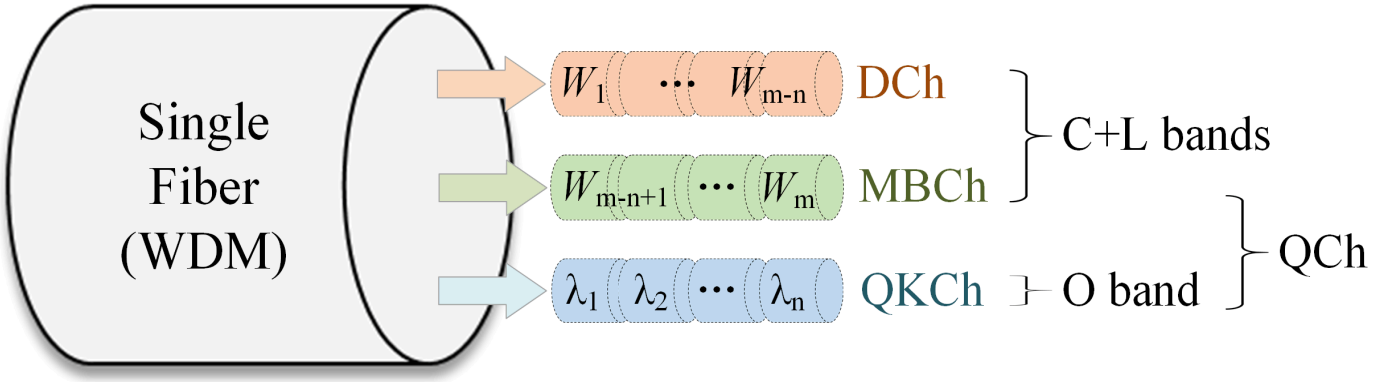
MBCh: part of wavelengths at C+L band, W_M in $W_{(C+L)}$ (assumed to be 4 in 40)

DCh: part of wavelengths at C+L band, W_D in $W_{(C+L)}$ (assumed to be 36 in 40)

Resource Map Construction Problem in QKD-ON

The wavelengths of QKCh and MBCh can be divided into many time slots (OTDM through fast switching, and each time slot can be different for different quantum key transmission, here assumed same ***t*** simply). Actually, there is latency for signaling, which is not considered here. Each request has different security priority, which is denoted with $\mathbf{T_r}$. $\mathbf{T_r}$ means that the quantum key ***r*** has to be updated in the period $\mathbf{T_r}$ ($t<\mathbf{T_r}$). $\mathbf{T_t}$ is the duration time of request ***r***. The switching latency is not considered neither.

$G(V,E)$
$r(s,d,T_r)$
N request number



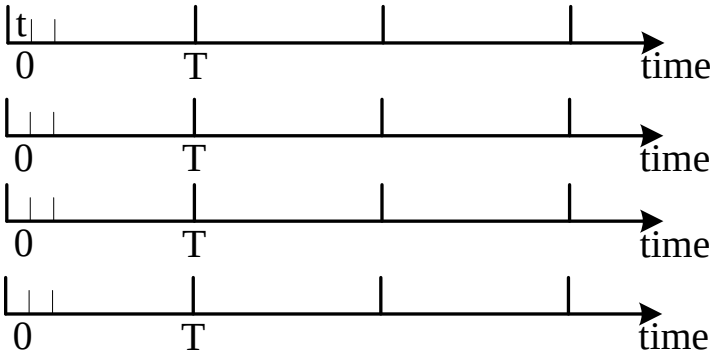
QKCh: wavelengths at O band, $\mathbf{W_O}$ (assumed to be 4), without considering distance.

MBCh: part of wavelengths at C+L band, $\mathbf{W_M}$ in $\mathbf{W_{(C+L)}}$ (assumed to be 4 in 40)

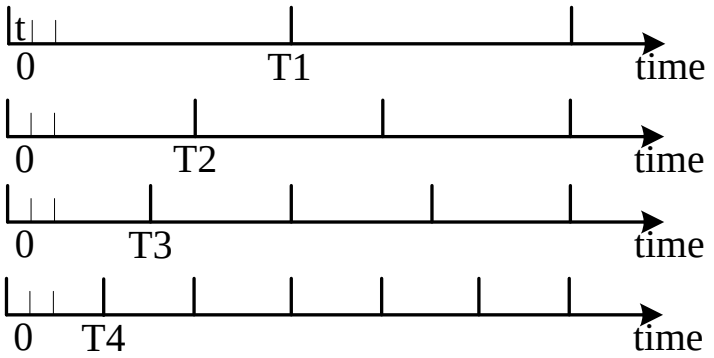
DCh: part of wavelengths at C+L band, $\mathbf{W_D}$ in $\mathbf{W_{(C+L)}}$ (assumed to be 36 in 40)

MBCh is synchronous with QKCh.

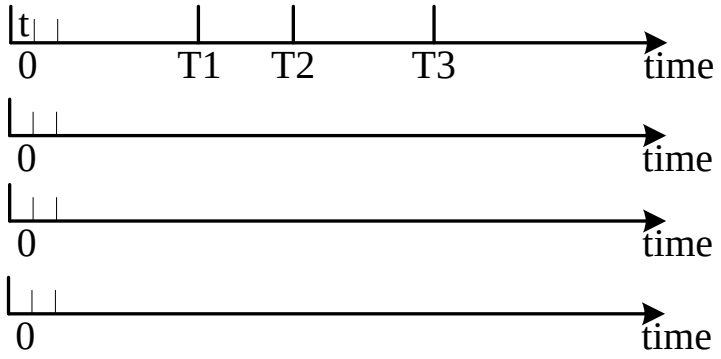
Resource Map Construction Problem in QKD-ON



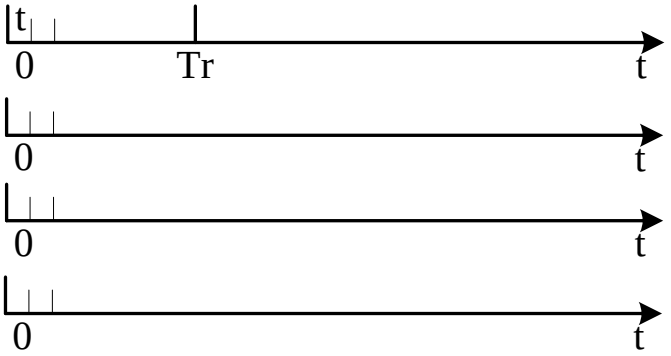
Case 1(fixed T for all wavelengths)



Case 2(fixed T for each wavelength)



Case 3(fixed T for each request)



Case 4(random T for each request)

t is the time for each request to lightpath switching and setup, and quantum key transmission, T is the time period of quantum key updating for each request.

Resource Map Construction Problem in QKD-ON

Static problem:

N is fixed, and there is no arrival and departure time for request r.

How to design the resource map with ILP and heuristic algorithm?

Dynamic problem:

N is not fixed, and service request follows Poisson distribution.

How to design the resource map with heuristic algorithm?

Variables: $\mathbf{t}$, $\mathbf{T_r}$, $\mathbf{T_t}$, $\mathbf{W_O}$, $\mathbf{W_M}$ ($=W_O$), $\mathbf{W_D}$, $\mathbf{W_{(C+L)}} = \mathbf{W_M}+\mathbf{W_D}$

Trade-off: *security priority and resource utilization (request number or connection security ratio)*

Resource Map Design Problem in QKD-ON, ILP-RWA

Given: $G(V,E)$, R, W_D

Object: $Min(\sum_{(l,k)\in E}\sum_{c\in R} w_{l,k,c})$

Variable:

c: node pair (source s_c and destination d_c)

$w_{l,k,r}$:number of wavelengths by link (l,k) assigned to request r, 0 or 1

v_c: number of connection requests having s_c as source node and d_c as destination node

A_l: set of all the nodes adjacent to node i

Constraints:

Wavelength number: $\sum_{c\in R} w_{l,k,c} \le W_D$

Wavelength continuity: $\sum_{k\in A_l} w_{k,l,c} - \sum_{k\in A_l} w_{l,k,c} = \begin{cases} v_c & if\ l = d_c \\ -v_c & if\ l = s_c \\ 0 & otherwise \end{cases} \quad \forall l,c$

Integrity: $w_{l,k,c}$

Resource Map Design Problem in QKD-ON, ILP-RWTA

Given: $G(V,E)$, R, t, T_r , W_O , W_M

Object: $Min(\sum_{(l,k)\in E}\sum_{w\in W_O}\sum_{c\in R}\tau_{(l,k,c,w)})$

Variable:

c: node pair (source s_c and destination d_c)

$w_{l,k,r}$:number of wavelengths by link (l,k) assigned to request r, 0 or 1

$\tau_{(l,k,r,w)}$: number of time slots by w on link (l,k) for request r, 0 or 1

v_c: number of connection requests having s_c as source node and d_c as destination node

A_l: set of all the nodes adjacent to node i

Constraints:

Wavelength number: $\sum_{c\in R} w_{l,k,c} \le W_D$

Wavelength continuity: $\sum_{k\in A_l} w_{k,l,c} - \sum_{k\in A_l} w_{l,k,c} = \begin{cases} v_c & if\ l = d_c \\ -v_c & if\ l = s_c \\ 0 & otherwise \end{cases} \quad \forall l,c$

Integrity: $w_{l,k,c} \quad t_{(l,k,c,w)}$

Time period: $\sum_{c\in R} \tau_{(l,k,c,w)} \le T$

Resource Map Design Algorithm in QKD-ON

Two use cases:
data request and QK request are separated or together.

Routing algorithm:
Dijkstra or KSP

Wavelength allocation algorithm:
First fit or Random fit

Time slot allocation algorithm:
First fit

Simulation work to be done

Blocking probability:

Wavelength utilization for data channel:

Connection security ratio:

Resource utilization for quantum channel:

Thank you for your attention!

Yongli Zhao

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