applied sciences

MDPI

Article

Multi-Dimensional Routing, Wavelength, and Timeslot Allocation (RWTA) in Quantum Key Distribution Optical Networks (QKD-ON)

Xiaosong Yu [1,2], Xian Ning [1], Qingcheng Zhu [1], Jiaqi Lv [1], Yongli Zhao [1,*], Huibin Zhang [1] and Jie Zhang [1]

[1] State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications (BUPT), Beijing 100876, China; xiaosongyu@bupt.edu.cn (X.Y.); lululu@bupt.edu.cn (X.N.); qingcheng@bupt.edu.cn (Q.Z.); lv_jiaqi@bupt.edu.cn (J.L.); zhanghuibin@bupt.edu.cn (H.Z.); lgr24@bupt.edu.cn (J.Z.)

[2] Science and Technology on Communication Networks Laboratory, Shijiazhuang 050081, China

* Correspondence: yonglizhao@bupt.edu.cn; Tel.: +86-010-61198108

Abstract: Currently, with the continuous advancement of network and communication technology, the amount of data carried by the optical network is very huge. The security of high-speed and large-capacity information in optical networks has attracted more and more attention. Quantum key distribution (QKD) provides information-theoretic security based on the laws of quantum mechanics. Introducing QKD into an optical network can greatly improve the security of the optical network. In order to reduce the cost of deployment on QKD infrastructure, quantum signals in QKD and classical signals in optical networks are multiplexed in the same fiber by wavelength-division manner. Moreover, due to the limited wavelength resources in an optical fiber, time-division technology is adopted to construct different kinds of channels in QKD system for efficient utilization of wavelength resources. Under such situation, how to satisfy the security requirements of service requests and complete the efficient scheduling of multi-dimensional resources, i.e., wavelengths and timeslots, is a challenging problem. This paper addresses this problem by considering multi-dimensional routing, wavelength, and timeslot allocation (RWTA) in short-distance quantum key distribution optical networks (QKD-ON), in which any two nodes can directly establish a quantum channel, and the maximum distance between any two nodes is less than the distance that can carry out point-to-point quantum key distribution process. While accommodating services with security requirements in QKD optical networks, to avoid the wavelength time-slot fragmentation caused by the constraints of wavelength consistency and time-slot continuity, we propose a time-window-based security orchestration strategy as well as relative-loss of time continuous compactness based RWTA strategy. We conducted the simulations under various scenarios, e.g., different key updating periods and different distributions on wavelength resources, etc., and the results show that the proposed strategy can achieve better performance compared with the baselines in terms of key success rate, key-updating delay, and blocking probability.

Keywords: optical network; RWTA; quantum key distribution

Citation: Yu, X.; Ning, X.; Zhu, Q.; Lv, J.; Zhao, Y.; Zhang, H.; Zhang, J. Multi-Dimensional Routing, Wavelength, and Timeslot Allocation (RWTA) in Quantum Key Distribution Optical Networks (QKD-ON). *Appl. Sci.* **2021**, *11*, 348. https://doi.org/

Received: 4 November 2020
Accepted: 28 December 2020
Published: 31 December 2020

1. Introduction

Quantum key distribution (QKD) is an advanced cryptographic technology which can provide unconditionally secure shared keys for separated users based on the basic laws of quantum mechanics [1]. The first QKD protocol, i.e., BB84 protocol, was proposed by Bennett and Brassard in 1984, and its security was verified in 2000 [2]. Different kinds of QKD networks based on beam splitters, optical switches, trusted repeaters, etc., have been successfully built and demonstrated [3–8]. Meanwhile, the improvement of quantum-signal transmission distance and key generation rate have promoted QKD to become practical.

As the physical transport layer of communication systems, optical networks accommodate data for various applications such as cloud computing, internet services, and so on.

The security of high-speed and large-capacity information transported in optical networks must be guaranteed. Several works have been dedicated to applying QKD technology to provide security solutions for optical networks [9–12]. In order to avoid the mutual interference of quantum signals and classical signals, a physical dedicated fiber was used for QKD at the beginning. That means quantum signals as well as classical signals are transmitted in different single-mode fibers respectively. However, this led to a significant waste of fiber resources and resulted in a relatively high cost. To solve this problem, a multiplexing manner, i.e., quantum signals and classical signals multiplexed into the same fiber, was proposed. Existing studies show that by adopting wavelength division multiplexing (WDM) technology and implementing proper wavelength isolation as well as wavelength filtering, quantum signals and classic signals can coexist in the same fiber [13–18].

Although the point-to-point quantum key distribution distance is limited, with the continuous expansion of the quantum key distribution network and the increasing number of users, quantum key distribution has been able to achieve long-distance encrypted communication [19,20]. The point-to-point QKD system for secure data transmission in optical networks is illustrated in Figure 1a [21]. This is the basic theoretical model of the paper. Alice and Bob configure shared quantum keys for data encryption and decryption on a traditional data channel (TDCh) through a quantum-key channel (QKCh) and a measurable-basis channel (MBCh), which will hereinafter be referred to as key configuration process. QKCh transmits photonic signals with different polarization quantum states, while MBCh sends synchronized clock signals and exchanges measurable-basis information. MBCh and TDCh can be digitally multiplexed together and then share the same wavelengths. Considering MBCh needs to maintain synchronization with QKCh, we assign proprietary wavelengths to build MBCh. Proper wavelengths are reserved for constructing these three types of channels, and then they are multiplexed into the same fiber by WDM technology. By using a nearly optimal wavelength allocation technique, the background noise caused by Raman on the quantum channel can be minimized, thereby maximizing the key generation rate that the quantum channel can achieve [22]. Figure 1b shows an example of wavelengths allocation for different channels on the C-band. By using higher frequency for QKCh, it can reduce Raman scattering effects [23], and reserve a large guard-band (e.g., 200 GHz) between QKCh and other channels to weaken four-wave-mixing effects [16]. Several different solutions are proposed to transport quantum signals and classical signals together over a single fiber. Ref. [24] shows that the best transmission performance of quantum signals was achieved in the C-band. It suggested the QKCh can be located at the highest frequency in the C-band and should have a large guard band between TDCh and MBCh [18]. Our previous work [21] researched the RWTA methods under the scenario that quantum signals and classical signals coexist in C-band in which 2, 4, and 6 wavelengths are allocated for QKCh and MBCh. Meanwhile, excluding the four wavelength channels reserved as guard band for QKCh and MBCh, 32, 28, and 24 allocated wavelengths remain for TDCh. There is also research to explore using O-band and C-band for carrying quantum signals and classical signals, respectively [14,15].

As described above, integrating QKD into optical networks can avoid the high cost of establishing dedicated QKD networks, which is a feasible and effective way to accommodate many more users in secure data communication. Some hybrid networking architectures based on trusted repeaters and weakly trusted repeaters have been proposed to overcome the transmission distance limit of quantum signals. Additionally, QKD-enabled optical network architecture supported by software-defined networking (SDN) has been demonstrated. Under the architecture, the unified construction of three types of channels mentioned above was discussed in detail [25,26]. Since wavelength resources in an optical fiber are limited, only a few wavelengths can be allocated to construct QKCh and MBCh. A timeslot slicing scheme based on optical time-division multiplexing (OTDM) technology can be adopted to construct QKCh and MBCh for efficient wavelength utilization. Due to the introduction of OTDM technology, resource allocation in QKD-enabled optical networks includes routing, wavelength, and timeslot assignment (RWTA) for key

configuration processes in addition to traditional routing and wavelength assignment (RWA) for data transmission. Reasonable scheduling and efficient utilization of those multi-dimensional resources, i.e., wavelengths and time-slots, is a very important topic in QKD optical networks. The RWTA methods in traditional OTDM optical networks mainly solve the problem of RWTA for the traditional data channel. For example, Ref. [22] studies how to determine the RWTA that meets the given request with a specified bandwidth. In the QKD-ON, the RWTA method is not only oriented to classical data channels, but also to quantum-key channels and measurable-basis channels. Apart from that, to improve the security of the encrypted data when adopting the advanced encryption standard (AES), the secure key for a TDCh should be updated periodically. The RWTA algorithm in Ref. [21] was designed to allocate wavelength and time-slot resources for the three types of channels considering different security levels. Ref. [21] also gave the feasibility of adopting OTDM to allocate multiple QKChs and TDChs over the same wavelength. The OTDM in QKDN is realized based on the traditional optical switches which support fast switching. Ref. [27] proposed the RWTA problem for efficient quantum key pool construction over WDM networks combining with quantum key pool (QKP) technique. However, they did not consider the wavelength-time-slot fragmentation caused by the constraints of wavelength consistency and time-slot continuity which this paper considers for improving the use of wavelength resources.

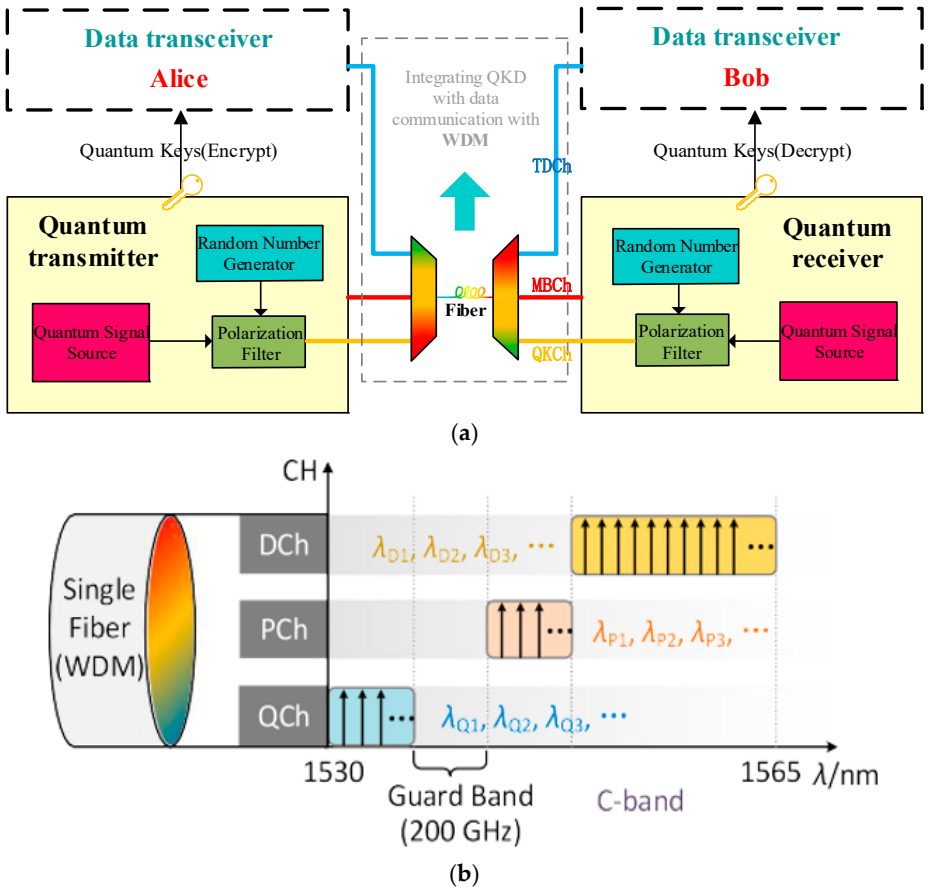


Figure 1. (**a**) Point-to-point quantum key distribution (QKD) system; (**b**) Wavelength allocation for different channels on C-band.

In this paper, we focus on the designing of resource allocation schemes for those three kinds of channels mentioned above. The main contributions in this work are as follows: (1) a time-window-based security orchestration (TW-SO) strategy for key updating is proposed to provide customized policies for services with different security levels. (2) Several indices

to describe the resource states are designed, including time continuous compactness and relative-loss of time continuous compactness. (3) The ReLoss-TCC (relative loss of time continuous compactness)-based multi-dimensional RWTA strategy is proposed while accommodating services with security requirements in QKD optical networks. It avoids the wavelength time-slot fragmentation caused by the constraints of wavelength consistency and time-slot continuity. (4) The simulation results show that the proposed strategy can achieve better performance compared with the baselines in terms of key success rate, key-updating delay, and blocking probability.

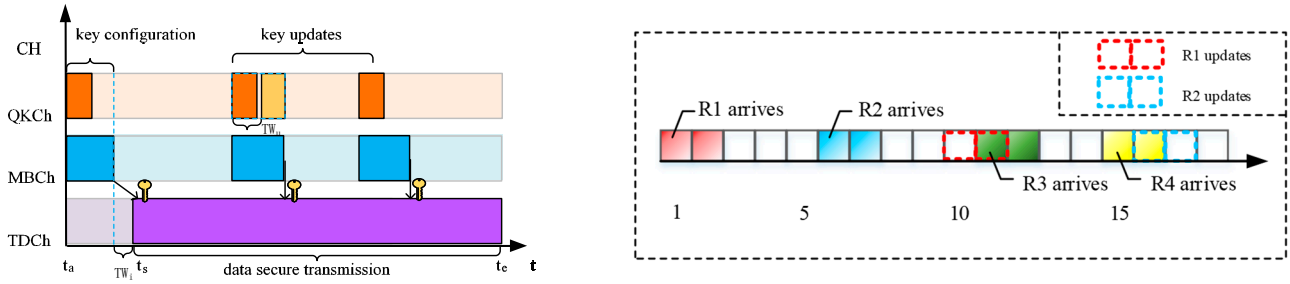
The rest of this paper is organized as follows. Section 2 describes the problem of resource allocation in QKD optical networks. A time-window-based security orchestration (TW-SO) strategy is designed in Section 3. The concept of time continuous compactness (TCC) is introduced. Based on the RWTA algorithm in Ref. [21], we further consider the limitation of the wavelength resources for quantum-key channels (QKChs). Our paper optimizes the allocation of QKChs and proposes a new ReLoss-TCC based RWTA strategy for avoiding the wavelength-time-slot fragmentation in Section 4. In Section 5, we design a multi-dimensional RWTA algorithm based on TW-SO and TCC-based RWTA for data secure transmission. Section 6 shows the simulation results over different scenarios. Finally, Section 7 concludes this paper.

2. Problem Statements

While accommodating services with security requirements in QKD optical networks, three kinds of channels, i.e., TDCh, QKCh, and MBCh, are involved. Scheduling those channels is essential to achieve secure data transmission for services. Figure 2a illustrates the coordination of the channels during secure communication. t_e represents the time when the data transmission ends. When the service request arrives, it is necessary to reserve a time window for key configuration [25]. Only after completing the key negotiation on QKCh and MBCh will the transmission of secure data on TDCh get start. The security of data transmission can be further enhanced by periodically updating the shared keys between communication parties. As can be seen from Figure 2a, different keys are negotiated through cooperation of QKCh and MBCh for data encryption and decryption on TDCh in different periods. We design security strategies by taking full advantage of the key update feature to satisfy the multi-security-level needs of various services. Several security-level provisioning solutions based on the key-updating period (such period is denoted as T hereafter) have been proposed based on the principle that services with higher security level require more frequent and flexible key updating [21]. Preventing the eavesdropping attacks on a transmission link plays a critical role in securing the safety of quantum-based algorithms. There has been research studying how to prevent such attacks [28], but the detailed discussion is beyond the scope of the paper. Note that the key-updating period is the period after which the secret key has to be changed between two parties, which can reduce the probability of key being cracked. There are two different schemes of key updating. One is updating keys for every definite period; the other is updating keys for every definite amount of data. The shorter definite period or the smaller definite amount of data means the higher security level. The selection of the key updating times is dependent on the speed of the TDCh and the security level required by the service. The details of selecting the key updating times are beyond the scope of this manuscript.

However, updating keys periodically is equivalent to multiplying the number of key configurations, which aggravates the load on QKCh and MBCh. In the case of limited wavelength resources, conflict on QKCh and MBCh occurs frequently in the process of RWTA. Since the resource allocations on QKCh and MBCh are synchronized, as shown in Figure 2a, we could only consider how to avoid the conflict on QKCh as a representative situation. Figure 2b illustrates the potential collision on QKCh due to dynamic service arrival, wavelength resource sharing, and key updating. The vertical axis in the figure represents the timeline, and the horizontal axis shows the timeslot of a certain wavelength belonging to QKCh. The timeslots occupied by different services are represented by small

grids of different colors. We try to assign #10 and #11 timeslots for key update when service R3 arrives at time 11. Conflict may occur since #11 timeslot has been assigned to key update request of R1. Similar conflict will occur at #16 timeslot obviously. The latency tolerance of key update configuration must be taken into account to avoid such conflicts in the RWTA process. In addition, if the communication between two nodes passes through an intermediate node, the intermediate node uses the bypass method. Consequently, the establishment of the quantum channel and data transmission between the nodes needs to meet wavelength consistency and timeslot continuity. Due to these constraints in RWTA, the wavelength-time-slot fragmentation problem will occur. Thus, how to maintain the connectivity of the paths in the process of RWTA is a very important research topic.



(**a**) (**b**)

Figure 2. (**a**) Coordination of three kinds of channels; (**b**) Resource allocation conflicts in routing, wavelength, and timeslot allocation (RWTA).

3. Time-Window-Based Security Orchestration

Providing customized policies for services with different security levels is one of the key points to improve the performance of QKD-enabled optical networks. As mentioned before, different security requirements for services can be satisfied by setting different key update period. The shorter the key update period is, the higher security levels can the service achieve. Since the secure keys are changed more frequently, it will increase the difficulty of acquiring the secure keys for the eavesdropper. There are two different kinds of key requests in the process of secure data communications. One is the key provisioning request, which is generated when security service arrives; another is the key updating request, which is generated to improve security level during secure data transmission. We define the accepted delay range of key provisioning request and key updating request as initial time window (TW_i) and update time window (TW_u), respectively. The value of TW_i and TW_u is determined by the latency range of service. As shown in Figure 2a, the non-immediate service arrives at t_a, and it only needs to transmit data before the deadline t_s, thus a period from t_a to t_s can be obtained for the key configuration process. Obviously, the latency range of service must be larger than the key configuration time, and TW_i is equal to the latency range of service minus the key configuration time. Different from TW_i, TW_u is related to the security levels of service requests. When there are multiple key updating requests, we can orchestrate them to acquire a reasonable deployment of key configuration channels (i.e., QKCh and MBCh) in time dimension. In this paper, a time-window-based security orchestration (TW-SO) strategy for key updating is proposed. When a key updating request is inserted into the queue, any request whose security level is lower will automatically slide backward within TW_u to satisfy the time delay. Suppose the key updating request is denoted as $r(s, d, t_a, TW_u, t, l)$, where s and d are the source and destination nodes, t_a is the key-updating time, TW_u is the update time window, l is the security level, t represents the time required to complete the key configuration; and then the process of TW-SO is shown in details in Algorithm 1.

Algorithm 1. Time-window-based security orchestration (TW-SO) strategy.

1 Request $r(s, d, t_a, TW_u, t, l)$ arrives;
2 Place $r(s, d, t_a, TW_u, t, l)$ to the last position of the key request queue;
3 ***For*** each request $r'(s', d', t_a', TW_u', t', l')$ in the key request queue which is in front of $r(s, d, t_a, TW_u, t, l)$
4 ***If*** $l > l'$ && $t_a < t_a' + TW_u'$
5 Exchange the positions of $r(s, d, t_a, TW_u, t, l)$ and $r'(s', d', t_a', TW_u', t', l')$;
6 ***End If***
7 ***End For***

4. Time Continuous Compactness Based *RWTA*

In the short-distance QKD-ON scenario, any two nodes can directly establish a quantum channel and the maximum distance between them is less than the distance that can carry out point-to-point quantum key distribution process. Consequently, the establishment of the quantum channel and data transmission between the nodes which are not connected directly needs to meet wavelength consistency and time continuity. The operation of RWTA for QKCh and MBCh must consider the effect on connectivity of wavelength-timeslots on the path. Otherwise, it will cause wavelength-timeslot fragments, which is not conducive to the efficient utilization of resources. An example of wavelength-timeslot fragments in RWTA is illustrated in Figure 3. Suppose path 2 (5-6-7-8) is the selected route for the request. When performing wavelength-timeslot allocation with 2 timeslots requirements over this route, the available timeslots with the smallest index would be allocated by using first-fit (FF) policy. In this paper, we consider three possible solutions when time-slots #3 and #4 are allocated on wavelengths λ1, λ2, and λ3, which are shown by the dotted rectangles of different colors in Figure 3a. Different solutions will have different impacts on other paths that share links with path 2. If solution A is selected, as illustrated in Figure 3b, the connectivity of timeslots from #1 to #4 on λ1 of path 3 is broken due to link #8 is being shared by path 3 and path 2. If a new request that needs 3 timeslots and starts transmitting before #4 timeslot arrives on path 3, it will be blocked since no eligible timeslots can be found. A similar problem arises while choosing solution B, as illustrated in Figure 3c. However, solution C, as illustrated in Figure 3d, does not break the wavelength-timeslot connectivity of path 1 and path 2. In order to reduce the blocking probability of subsequently arriving requests, solution C should be chosen as the final wavelength-timeslot allocation.

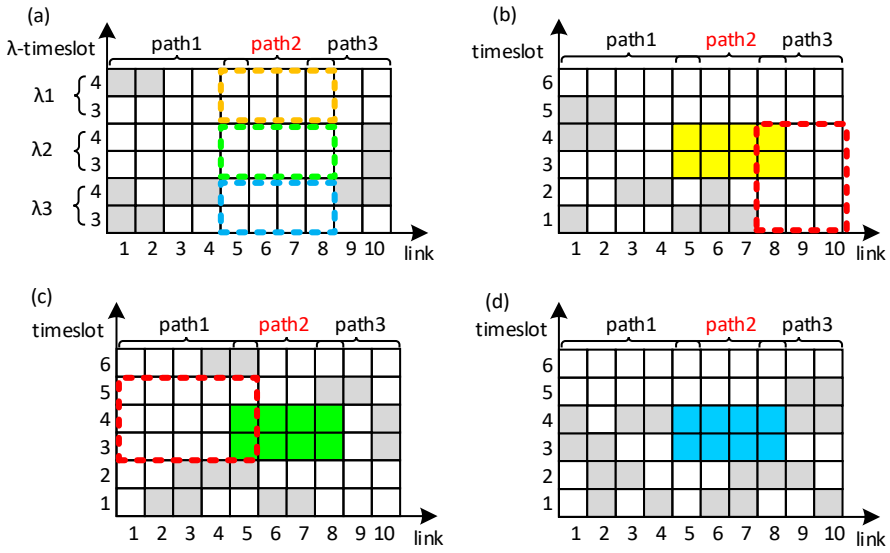


Figure 3. An example of wavelength-timeslot fragments in RWTA: (**a**) Three possible solutions on wavelengths λ1, λ2, and λ3; (**b**) Resource status on λ1 after solution A; (**c**) Resource status on λ2 after solution B; (**d**) Resource status on λ3 after solution C.

Therefore, a reasonable RWTA scheme should try its best to guarantee that the resource connectivity on each path is not damaged. In order to avoid the fragments of wavelength-timeslot resources, this paper introduces the concept of time continuous compactness (TCC), which is used to describe the connectivity of wavelength resources on the links of each path in a time dimension. Furthermore, a relative loss of time continuous compactness (ReLoss-TCC)-based RWTA strategy is proposed.

4.1. Time Continuous Compactness (TCC)

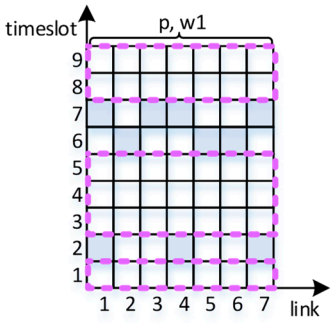
We define C_{φ}^{pw} as the TCC of wavelength w on path p in $[t_s, t_e]$ in φ state, as shown in Equation (1). φ denotes the state of network, K_{φ}^{pw} indicates the number of available timeslot segments at wavelength w on path p in φ state, and N_{φ}^{pwj} represents the number of timeslots on available timeslot segment j at wavelength w on path p in φ state. From the definition, we can see that the larger C_{φ}^{pw} is, the better connectivity of wavelength-timeslots on the path will be.

$$C_{\varphi}^{pw} = \frac{\sum_{j=1}^{K_{\varphi}^{pw}} N_{\varphi}^{pwj}}{(t_e - t_s) + 1} \cdot \frac{1}{K_{\varphi}^{pw}} \tag{1}$$

Let W denote the set of wavelengths on path p. In φ state, TCC of path p in period $[t_s, t_e]$ is represented by C_{φ}^{p}, which is the sum of TCC of all wavelengths on p, as defined in Equation (2). Small C_{φ}^{p} means that the path has poor wavelength-timeslots connectivity during this period, possibly due to heavy traffic carried on the path or large number of wavelength-timeslot fragments on the path. Under such situation, if new service requests arrive on path p, the probability of being blocked will be relatively high.

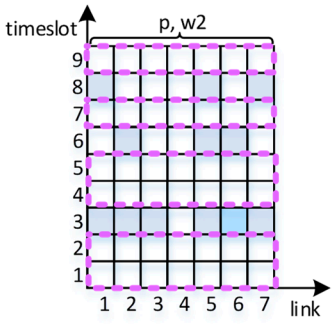
$$C_{\varphi}^{p} = \sum_{w \in W} C_{\varphi}^{wp} \tag{2}$$

Figure 4 gives an illustrating example of TCC calculation. In the figure, the grids with color represent the occupancy of timeslots on path p in φ state, and the grids without color indicate that they are available. Timeslots enclosed in dotted rectangles indicate that they are connective on the path. By calculating TCC of two wavelengths in the timeslot segment, TCC of $w1$ is larger than that of $w2$. Obviously, the connectivity of timeslots for $w1$ is better than $w2$ on path p.



$$C_{\varphi}^{pw_1} = \frac{1+3+2}{(9-1)+1} \times \frac{1}{3} = \frac{2}{9}$$

(**a**)



$$C_{\varphi}^{pw_2} = \frac{2+2+1+1}{(9-1)+1} \times \frac{1}{4} = \frac{1}{6}$$

(**b**)

Figure 4. (**a**) Time continuous compactness (TCC) on wavelength $w1$; (**b**) TCC on wavelength $w2$.

4.2. Relative-Loss of Time Continuous Compactness (ReLoss-TCC)

Wavelength-timeslot allocation on a path in QKD optical network will have a great impact on resource connectivity of this path as well as other paths that share links with it. Therefore, when evaluating the influence of RWTA schemes on network resource status, not

only the TCC on the path but also the TCC on other paths sharing links with this path need to be considered. In QKD optical networks, in order to save costs, the quantum devices such as quantum signal generators, quantum measurement devices, etc., are deployed only at nodes that have security requirements, and the routes for services are determined in advance. This means that static routing scheme is suitable for the RWTA process. Suppose $P(p)$ denotes the set of paths that share links with p, then the TCC of $P(p)$ in φ state is shown as follows.

$$C_{\varphi}^{P(p)} = \sum_{p \in P(p)} C_{\varphi}^{p} \tag{3}$$

We jointly consider C_{φ}^{p} and $C_{\varphi}^{P(p)}$ to evaluate the influence of specific RWTA scheme on the connectivity of network resources in time dimension, and propose a relative-loss of time continuous compactness (ReLoss-TCC)-based RWTA strategy. ReLoss-TCC is used to describe the relative changes of TCC after wavelength-timeslot allocation, and the definition is shown in Equation (4). Here, φ denotes the network state before wavelength-timeslot allocation, while φ' denotes the network state after wavelength-timeslot allocation.

$$ReLoss\text{-}TCC \frac{\left(C_{\varphi}^{P(p)} - C_{\varphi'}^{P(p)}\right) + \left(C_{\varphi}^{P} - C_{\varphi'}^{P}\right)}{C_{\varphi}^{P(p)} + C_{\varphi}^{P}}, \tag{4}$$

4.3. ReLoss-TCC-Based RWTA Strategy

The RWTA strategy based on ReLoss-TCC refers to the routing and wavelength-timeslot solution which minimizes the relative change of the TCC in all alternatives. That means it has the least impact on the connectivity status of network resources after the RWTA process. Suppose the request is denoted as $r(s, d, t_a, TW, t, l)$, where s and d represent the source node and destination node, t_a represents the arrival time of this request, TW represents the time window, t represents the number of timeslots required for the request, and l is the security level. The ReLoss-TCC-based RWTA strategy is shown in Algorithm 2 and specifically includes the following three stages: (i) network initialization and routes configuration (Step 1–5); (ii) find all alternative solutions for the arriving request based on FF strategy (Step 6–17); and (iii) get the final solution based on ReLoss-TCC strategy (Step 18–22).

Algorithm 2. ReLoss (relative loss)-TCC-based RWTA strategy.

1 Topology $G(V, E)$, Source and destination pairs $\{s, d\}$;
2 ***For*** each $\{s, d\}$ pair, **do**
3 calculate the shortest paths p;
4 store p into set P;
5 create map $\{s, d\} \rightarrow p$;
6 ***End For***
7 ***For*** each path p in set P, **do**
8 find the paths which share links with p, store them into set $P(p)$;
8 ***End For***
9 Request $r(s, d, t_a, TW, t, l)$ arrives;
10 Search the path p according to the map created in *step 2*;
11 Find the wavelengths of *QKCh* on path p that satisfy wavelength consistency constraint;
12 store the wavelengths into set W;
13 ***If*** $W \neq \varnothing$
14 ***For*** each w in set W
15 Search the available timeslots in $[t_a, t_a + TW + t]$;
16 store timeslots into set S;
17 ***If*** $S \neq \varnothing$
18 find the available timeslot segments with length t;
19 store timeslot into set WT;

```
            If WT ≠ ∅
                Select the timeslot segment with the lowest index in WT by FF strategy;
                calculate the value of ReLoss-TCC;
            End If
        End If
            Find the minimum value of ReLoss-TCC
            allocate the corresponding wavelength and timeslots for the request;
    End For
Else
        Block the request;
End If
```

5. Multi-Dimensional RWTA in QKD Optical Networks

Compared with traditional optical networks, routing and resource allocation in QKD optical networks includes RWTA conducted on QKCh and MBCh in addition to RWA conducted on TDCh. In this paper, we design a multi-dimensional RWTA algorithm to dynamically allocate resources for different channels, i.e., wavelength assignment for TDCh, and wavelength and time-slot assignment for QKCh and MBCh due to the wavelength consistency and time continuity the QKCh needs to meet. Suppose the service request in QKD optical networks is denoted as $r(s, d, t_a, TW_i, TW_u, t, l)$. When l equals to 0, it means that there is no security requirement for the request; otherwise, it needs to configure key-updating period T according to the value of l until the data transmission is finished. The proposed multi-dimensional RWTA in QKD optical networks is shown in Algorithm 3.

Algorithm 3. Multi-dimensional RWTA in QKD optical networks.

```
Request r(s, d, t_a, TW_i, TW_u, t, l) arrives;
Generate key initialization request r(s, d, t_a, TW_i, t, l);
Search the wavelength-timeslots for r(s, d, t_a, TW_i, t, l) according to ReLoss-TCC-based RWTA Strategy;
Search the available wavelengths for TDChs on path p;
store the wavelengths into set W;
If W ≠ ∅
    Allocate the wavelength for TDChs by FF strategy;
    Start the data transmission in TDChs;
    k = 1;
    While data transmission is not finished
        Select the value of T according to l;
          generate key updating request r(s, d, t_a + k * T, TW_u, t, l);
          insert into key-updating request queue Q by TW-SO Strategy;
        Search the wavelength-time-slots for requests in queue Q according to ReLoss-TCC-based RWTA Strategy;
          k = k + 1;
     End While
Else
    Block the request;
End If
```

6. Simulation Results and Discussions

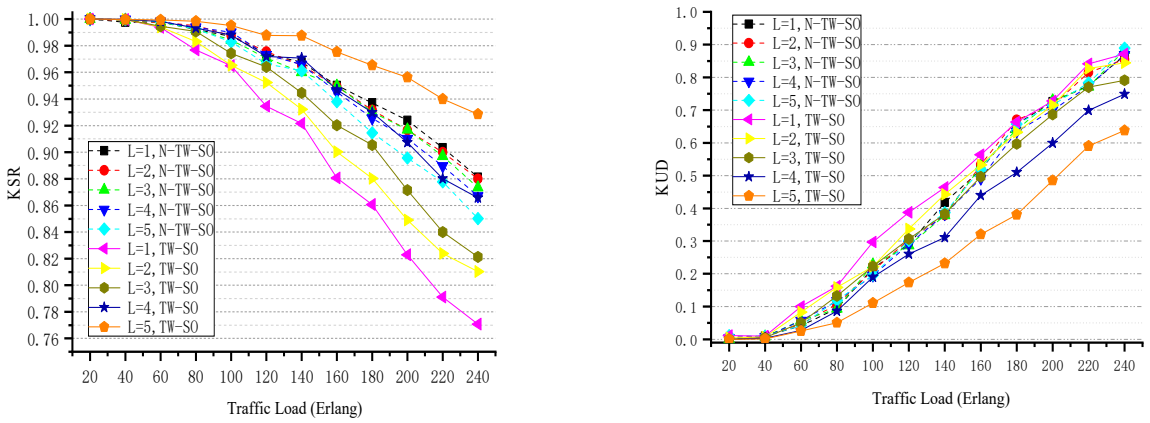
NSFNET topology with 14 nodes and 21 links was adopted for simulation to evaluate the performance of the proposed multi-dimensional RWTA algorithm. Our work focuses on short distance QKD-ON scenario. NSFNET topology's nodes and links were taken into this simulation and the maximum distance between any two nodes was less than the distance that can carry out point-to-point quantum key distribution process. Meanwhile, we assumed that the key generation rate of all links is constant. Forty wavelengths are considered in each fiber link according to the commercial systems. Multiplexing QKD and classical flows at different spectral windows (e.g., O-band, C-band) could be an option to overcome the contamination associated with Raman scattering. In future work, relevant research will be considered. Four wavelengths (200 GHz spectrum grid) are reserved as the

guard band between QKCh and the other two channels to avoid four-wave-mixing effects as mentioned before [24]. The number of wavelengths reserved for MBCh is assumed to be the same as QKCh. Service requests are randomly generated among all node pairs following Poisson distribution. To the best of our knowledge, for the RWTA problem in QKD-ONs, Ref. [21] has proposed the RWTA algorithm considering three types of channels and different security levels of services which is a basic work. This paper considers how to improve the wavelength utilization under the fixed updating period scenario based on the theoretical model proposed in Ref. [21]. Therefore, we chose the first-fit (FF) based RWTA strategy in Ref. [21] for comparison in our paper. In addition, for learning more about the performance of our proposed algorithm, we also took the random-fit (RF) based RWTA strategy as comparison. The simulation is composed of three parts: (1) the performance of TW-SO strategy for provisioning of multi-security-level services is verified; (2) the performance of ReLoss-TCC-based RWTA strategy in different scenarios is demonstrated; (3) the performance of multi-dimensional RWTA algorithm for three different kinds of channels under different wavelength assignment scenarios are explored.

6.1. TW-SO Strategy for Provisioning of Multi-Security-Level Services

We assume that the unit key generation rate of each time-slot is set to a fixed value. To verify the performance of TW-SO strategy, different key-updating periods T, i.e., 50, 70, 90, 110, 130 timeslots) were configured for service requests with different security levels. Four wavelengths were assigned to QKCh, and the QKCh of each wavelength was divided into 200 fixed-size timeslots. The number of timeslots required for the request t was randomly generated from [5,10], and the update time window TW_u was set to 3 timeslots. The key success rate (KSR) and key-updating delay (KUD) were evaluated for provisioning of multi-security-level services in the simulation. Non-TW-SO (N-TW-SO) strategy was used as the baseline to compare the performance of TW-SO strategy.

The results of KSR and KUD are illustrated in Figure 5a,b, respectively. From those two figures we can clearly see that, for N-TW-SO strategy, the KSR decreased as the security level increased, but there was no difference in KUD among different security levels. The reason is that for a higher security level request, smaller T should be configured, which then leads to more consumption of wavelength-timeslots resources, thus resulting in lower KSR finally. However, for KUD, they keep the same values since there are no priority considerations on security level under N-TW-SO strategy. Obviously, this cannot hit the mark of providing multi-level secure transmission over QKD optical networks. In contrast, for TW-SO strategy, higher security level requests can obtain higher KSR and lower KUD. That means that the TW-SO strategy can not only meet the requirements of multi-level secure data provisioning, but also reduce the blocking probability brought by the frequently key-updating process.



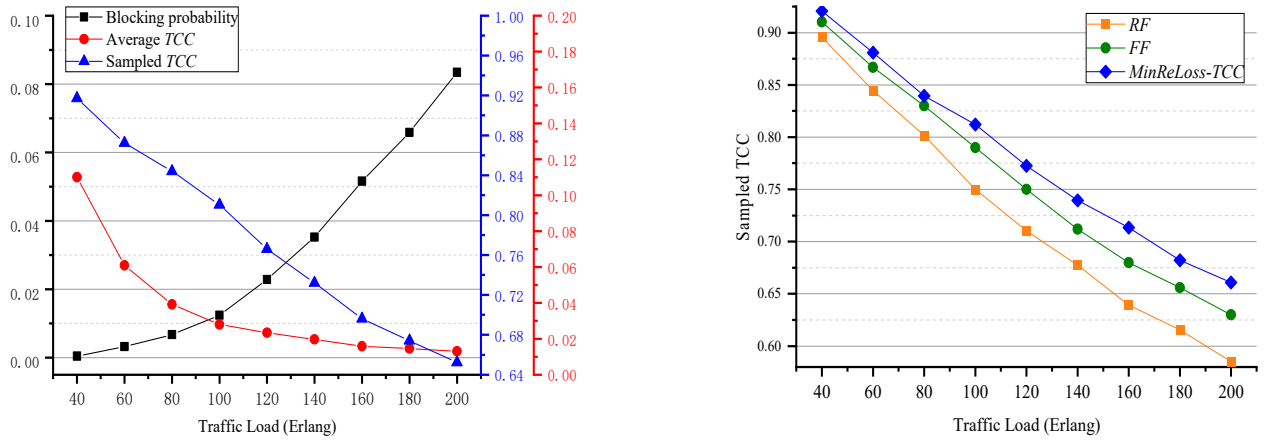
(**a**) (**b**)

Figure 5. (**a**) Key success rate (KSR) vs. traffic load; (**b**) Key-updating delay (KUD) vs. traffic load.

6.2. ReLoss-TCC-Based RWTA Strategy in Different Scenarios

In this section, we try to find the effect of TCC on the performance of blocking probability under ReLoss-TCC-based RWTA strategy in QKD optical networks. Two kinds of TCC, i.e., average TCC and sampled TCC, are introduced in this part. Average TCC is defined as the average value of TCC calculated right after accommodating each request in the simulation, while sampled TCC refers to the average value of TCC calculated by sampling network wavelength-timeslots status in range $[t_a,\ t_a + t_0]$ after accommodating each request. Here, t_a is the arrival time of request and t_0 is a constant corresponding to the sample strategy. The main difference between them is that for sampled TCC, services which are accommodated in the network may come to an end during $[t_a,\ t_a + t_0]$ and thus release the wavelength-timeslot resources, resulting in a different value of TCC. In this section, four wavelengths are assigned for QKCh and MBCh respectively, and the number of required timeslots is randomly generated among [5,15] timeslots. In addition, TW_u is set to be 3 timeslots, and t_0 is set to be 10 timeslots.

Figure 6a indicates the relationship among average TCC, sampled TCC, and blocking probability. From these curves we can see that, as the traffic load increased, the sampled TCC decreased uniformly, and the blocking probability increased uniformly. However, for average TCC, it dropped significantly when the traffic load increased lightly and remained relatively low when the traffic load continued to increase. Then, we evaluate the sampled TCC for three different RWTA strategies, i.e., ReLoss-TCC-based RWTA strategy, random-fit (RF)-based RWTA strategy and first-fit (FF)-based RWTA strategy under different traffic loads, as shown in Figure 6b. RF-based RWTA strategy refers to the random selection among all alternative wavelength-timeslot segments, while FF-based RWTA strategy selects the available wavelength-timeslot segments with the lowest index. From the results we can clearly concludes that among these three candidates, ReLoss-TCC-based RWTA strategy achieved the best performance, followed by FF-based RWTA strategy, and lastly RF-based RWTA strategy.



(**a**) (**b**)

Figure 6. (**a**) Relationship among average TCC, sampled TCC, and blocking probability; (**b**) Sampled TCC under ReLoss-TCC-based RWTA, RF-based RWTA, and FF-based RWTA strategy.

To further verify the relationship between sampled TCC and provisioning capability of the network, we display the blocking probabilities of ReLoss-TCC-based RWTA strategy, RF-based RWTA strategy, and FF-based RWTA strategy under different traffic loads, as shown in Figure 7a. Combined with Figure 6b, we can see that higher value of sampled TCC will achieve lower blocking probability in the network, and vice versa. This confirms the previous conclusion we got from Figure 6a. Moreover, in order to explore the performance of RWTA strategy under different scenarios, two kinds of timeslot requirements were

configured for key requests. One is the requirements of requests are diverse, and they are randomly chosen from [5,15] timeslots; another is the requirements are constant, and they are fixed to 10 timeslots. For the former scenario, ReLoss-TCC-based RWTA strategy got the lowest blocking probability, and the gaps between different strategies were obvious. For example, when the traffic load is 160 Erlang, the ReLoss-TCC-based RWTA strategy can obtain 29.69% and 20.35% reduction compared to RF-based RWTA strategy and FF-based RWTA strategy respectively, as shown in Figure 7a. However, for the later scenario, the gaps in blocking probabilities of those three strategies were not prominent, with ReLoss-TCC-based RWTA strategy performing slightly better under most of the traffic loads, as shown in Figure 7b. This indicates that the proposed ReLoss-TCC-based RWTA strategy is more applicable to the scenarios with diverse timeslots requirements.

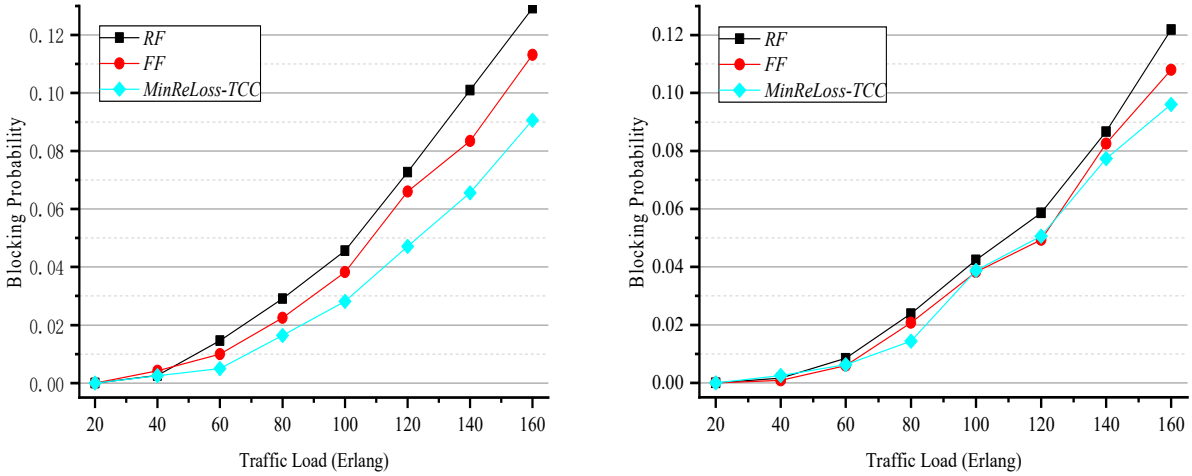


Figure 7. (**a**) Blocking probability vs. traffic load when the requirements of timeslots are diverse; (**b**) Blocking probability vs. traffic load when the requirements of timeslots are constant.

6.3. Multi-Dimensional RWTA for Different Kinds of Channels

As described above, there are three different kinds of channels, i.e., TDCh, QKCh and MBCh in QKD optical networks. Setting up QKCh and MBCh for key configuration will enhance the security, but it also brings wavelength-timeslots consumption. How to balance the wavelength-timeslot resources that are allocated to those three channels is a very important topic. In this part, while establishing three channels, we apply the proposed multi-dimensional RWTA under three different cases. Three different cases include that the wavelengths allocated to TDCh, QKCh, and MBCh are 32:2:2, 28:4:4, and 24:6:6 respectively. Blocking probabilities of TDCh and QKCh in the network under three cases are shown in Figure 8a,b. It can be seen from the figures that the more wavelengths assigned to QKCh and MBCh, the higher blocking probability TDCh achieved, but lower blocking probability can be obtained by QKCh; and vice versa. One thing we need to notice is that by increasing 2 wavelengths (i.e., 5%) allocated to QKCh, the blocking probability of TDCh increased by 27.5% (under 240 Erlang traffic load), but the blocking probability of QKCh reduced up to 82.1%. This means that we could greatly improve the security level of requests at a relatively low cost of network provisioning capacity.

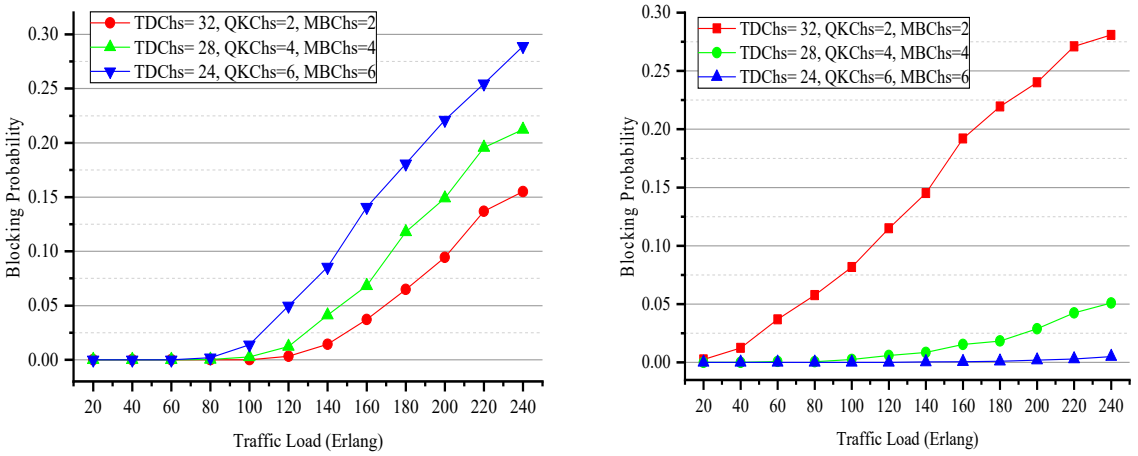


Figure 8. (**a**)Blocking probability of TDCh vs. traffic load; (**b**) Blocking probability of QKCh vs. traffic load.

7. Conclusions

This paper investigated the problem of multi-dimensional routing, wavelength, and timeslot allocation (RWTA) in time-division based quantum key distribution optical networks (QKD-ON). We have designed a time-window-based security orchestration (TW-SO) strategy. To enable efficient utilization of wavelength resources, a relative loss of time continuous compactness-based RWTA strategy was proposed. Simulation evaluations were conducted under different scenarios, e.g., different key updating periods and different distributions on wavelength resources. Based on the results, we can draw conclusions that in terms of key success rate, key-updating delay, and blocking probability, the proposed strategy can achieve better performance compared with the baselines. Meanwhile, it is more applicable to the scenarios with diverse timeslots requirements. Moreover, the relationship between security level and network provisioning capacity was discussed, and how to get a trade-off between them requires further study.

Author Contributions: Conceptualization, X.Y., X.N., and Y.Z.; methodology, X.Y. and Y.Z.; software, X.N.; validation, Q.Z. and J.L.; writing—original draft preparation, X.Y. and X.N.; writing—review and editing, Q.Z., J.L., Y.Z., H.Z., and J.Z.; supervision, J.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by NSFC project (*61971068, 61822105, and 61601052*), Fund of National Key Research and Development Program of China (2020YFE0200600), Fund of Science and Technology on Communication Networks Laboratory (*6142104180405*), Fund of State Key Laboratory of Information Photonics and Optical Communications, BUPT (*IPOC2020ZT04*, *IPOC2019ZR01*), Fund of State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, China (*2020GZKF012*), and the Fundamental Research Funds for the Central Universities (*2019XD-A05, 2018RC24*).

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
2. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]
3. Elliott, C. Building the quantum network. *New J. Phys.* **2002**, *4*, 46. [CrossRef]
4. Elliott, C.; Pearson, D.; Troxel, G. Quantum cryptography in practice. *arXiv* **2003**, *33*, 227–238.

5. Peev, M.; Pacher, C.; Alléaume, R.; Barreiro, C.; Bouda, J.; Boxleitner, W.; Debuisschert, T.; Diamanti, E.; Dianati, M.; Dynes, J.F.; et al. The SECOQC Quantum-Key-Distribution Network in Vienna. *New J. Phys.* **2009**, *11*, 075001. [CrossRef]
6. Dianati, M.; Alléaume, R.; Gagnaire, M.; Shen, X. Architecture and protocols of the future European quantum key distribution network. *Secur. Commun. Netw.* **2008**, *1*, 57–74. [CrossRef]
7. Horiuchi, N. View from. UQCC 2010: Quantum secure video. *Nat. Photonics* **2010**, *5*, 10–11. [CrossRef]
8. Fujiwar, M. Field Demonstration of Quantum Key Distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387.
9. Hirot, O. Quantum key distribution with unconditional security for all optical fiber network. *Proc. SPIE* **2003**, *5161*, 320–331.
10. Stucki, D.; Legré, M.; Buntschu, F.; Clausen, B.; Felber, N.; Gisin, N.; Henzen, L.; Junod, P.; Litzistorf, G.; Monbaron, P.; et al. Long term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **2011**, *13*, 123001–123018. [CrossRef]
11. Kitayama, K.-I.; Sasaki, M.; Araki, S.; Tsubokawa, M.; Tomita, A.; Inoue, K.; Harasawa, K.; Nagasako, Y.; Takada, A. Security in Photonic Networks: Threats and Security Enhancement. *J. Light. Technol.* **2011**, *29*, 3210–3222. [CrossRef]
12. Elkouss, D.; Martinez-Mateo, J.; Ciurana, A.; Martin, V. Secure optical networks based on quantum key distribution and weakly trusted repeaters. *IEEE OSA J. Opt. Commun. Netw.* **2013**, *5*, 316–328. [CrossRef]
13. Townsend, P. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing. *Electron. Lett.* **2002**, *33*, 188–190. [CrossRef]
14. Runser, R.J. Demonstration of 1.3 μm Quantum Key Distribution (QKD) Compatibility with 1.5 μm Metropolitan Wavelength Division Multiplexed (WDM) Systems. In Proceedings of the Optical Fiber Communication Conference, Optical Society of America, Anaheim, CA, USA, 6–11 March 2005.
15. Nweke, N.; Runser, R.; McNown, S.; Khurgin, J.; Chapuran, T.; Toliver, P.; Goodman, M.; Jackel, J.; Hughes, R.; Peterson, C.; et al. EDFA bypass and filtering architecture enabling QKD+WDM coexistence on mid-span amplified links. Conference on Lasers and Electro-Optics 2006. In Proceedings of the Quantum Electronics and Laser Science Conference, Long Beach, CA, USA, 21–26 May 2006; pp. 1–2.
16. He, L.; Niu, J.; Sun, Y.; Ji, Y. The four wave mixing effects in quantum key distribution based on conventional WDM network. In Proceedings of the International Conference on Optical Internet 2014 (COIN), Hyatt Regency Jeju, Korea, 27–29 August 2014; pp. 1–2.
17. Wang, L.-J.; Chen, L.-K.; Ju, L.; Xu, M.-L.; Zhao, Y.; Chen, K.; Chen, Z.-B.; Chen, T.-Y.; Pan, J.-W. Experimental multiplexing of quantum key distribution with classical optical communication. *Appl. Phys. Lett.* **2015**, *106*, 175–179. [CrossRef]
18. Peters, N.; Toliver, P.; Chapuran, E.T.; Runser, R.J.; McNown, S.R.; Peterson, C.G.; Rosenberg, D.; Dallmann, N.; Hughes, R.; McCabe, K.P.; et al. Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments. *New J. Phys.* **2009**, *11*, 045012. [CrossRef]
19. Liu, Y.; Chen, T.Y.; Wang, J. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express* **2010**, *18*, 8587–8594. [CrossRef]
20. Liao, S.K.; Cai, W.Q.; Liu, W.Y. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [CrossRef]
21. Zhao, Y.-L.; Cao, Y.; Wang, W.; Wang, H.; Yu, X.; Zhang, J.; Tornatore, M.; Wu, Y.; Mukherjee, A.B. Resource Allocation in Optical Networks Secured by Quantum Key Distribution. *IEEE Commun. Mag.* **2018**, *56*, 130–137. [CrossRef]
22. Wen, B.; Sivalingam, K.M. Routing, Wavelength and Time-Slot Assignment in Time Division Multiplexed Wavelength-Routed Optical WDM Networks. In Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, New York, NY, USA, 23–27 June 2002; Volume 3, pp. 1442–1450.
23. Kawahara, H.; Medhipour, A.; Inoue, K. Effect of spontaneous Raman scattering on quantum channel wavelength-multiplexed with classical channel. *Opt. Commun.* **2011**, *284*, 691–696. [CrossRef]
24. Bahrani, S.; Razavi, M.; Salehi, J.A. Optimal Wavelength Allocation in Hybrid Quantum-Classical Networks. In Proceedings of the 24th European Signal Processing Conference (EUSIPCO), Budapest, Hungary, 29 August–2 September 2016.
25. Cao, Y.; Zhao, Y.-L.; Yu, X.; Wu, Y. Resource assignment strategy in optical networks integrated with quantum key distribution. *IEEE Osa J. Opt. Commun. Netw.* **2017**, *9*, 995–1004. [CrossRef]
26. Cao, Y.; Zhao, Y.-L.; Colman-Meixner, C.; Yu, X.; Zhang, J. Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). *Opt. Express* **2017**, *25*, 26453–26467. [CrossRef] [PubMed]
27. Cao, Y.; Zhao, Y.-L.; Wu, Y.; Yu, X.; Zhang, J. Time-Scheduled Quantum Key Distribution (QKD) Over WDM Networks. *J. Light. Technol.* **2018**, *36*, 3382–3395. [CrossRef]
28. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Security of two-way quantum cryptography against asymm31etric Gaussian attacks. *Proc. SPIE* **2008**, *7092*, 709215.