applied sciences

Article

Quantum-Key-Distribution (QKD) Networks Enabled by Software-Defined Networks (SDN)

Hua Wang [1], Yongli Zhao [1,*] and Avishek Nag [2]

[1] State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China; Whua@bupt.edu.cn

[2] The School of Electrical and Electronic Engineering, University College Dublin, Dublin 999015, Ireland; avishek.nag@ucd.ie

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

Received: 18 April 2019; Accepted: 15 May 2019; Published: 21 May 2019

Featured Application: Authors are encouraged to provide a concise description of the specific application or a potential application of the work. This section is not mandatory.

Abstract: As an important support for quantum communication, quantum key distribution (QKD) networks have achieved a relatively mature level of development, and they face higher requirements for multi-user end-to-end networking capabilities. Thus, QKD networks need an effective management plane to control and coordinate with the QKD resources. As a promising technology, software defined networking (SDN) can separate the control and management of QKD networks from the actual forwarding of the quantum keys. This paper systematically introduces QKD networks enabled by SDN, by elaborating on its overall architecture, related interfaces, and protocols. Then, three-use cases are provided as important paradigms with their corresponding schemes and simulation performances.

Keywords: quantum key distribution (QKD); networks; soft-defined networking (SDN)

1. Introduction

With rapid developments in Internet of Things technology, more secure communication for users is required with increasing demands in information networks, so as to overcome perceived security threats as much as possible. As a promising technology, quantum key distribution (QKD) has been proven to provide users with secure keys exploiting the laws of quantum physics, i.e., Heisenberg's uncertainty principle and no-cloning theorem [1]. These features allow two users to know if there is any eavesdropping during the communication process between them [2]. To extend QKD for multiple users, QKD networks have been studied and developed around the world in the past decades, which mainly uses laying fibers as basic transmission medium to serve security demands with secret-key provisioning [3–5]. Furthermore, the construction of QKD backbones and metro-area networks currently has been launched with large investment, and their development is attracting great attention around world.

Traditional QKD is limited to point-to-point connectivity in the physical layer, using resources like wavelengths and time slices having different capacities depending on the point-to-point QKD demand. A QKD network however, needs the ability to allocate different resources in a global manner using a unified control plane for the easier operation. To address this problem, software-defined networking (SDN) has gained popularity by dividing networks into data plane and control plane and supporting programmability of network functionalities [6,7]. The core idea of SDN is to realize flexible control of traffic and make the network more intelligent by separating control and data planes. The control plane can grasp the global network view and make it convenient for operators to manage and upgrade the network efficiently. In the coming years, QKD networks enabled by SDN will be an important scenario for developing multi-user cases. On the one hand, QKD networks can be controlled by SDN for the unified interaction of network devices and protocols [8]; on the other, QKD can be a secure solution for SDN-based networks [9]. Therefore, there are some researches focused on the topics of QKD networks with SDN. A QKD-enabled optical network architecture is proposed to add an additional layer, i.e., QKD layer, for secret keys in software-defined optical networks (SDONs) [10]. Moreover, some key-assignment schemes are developed to secure control signals and data services and enhance their security in SDONs [11–13] with wavelength division multiplexing (WDM) [14] and optical time division multiplexing (OTDM) [15,16]. However, there is a lack of studies addressing systematic secret-key allocation with centralized control and coordination of the QKD resources.

In this paper, by introducing SDN technology into the management of QKD networks, we carefully described the architecture of QKD networks enabled by SDN, including available interfaces and protocols in the networks. To solve three important issues in QKD networking, we have designed multi-resources allocation, secret-key management and survivability guarantee to provide reference results. To explain these with specific details, we have structured the paper as follows. Section 2 introduces recent progresses of QKD networks, and Section 3 describes the architecture of QKD networks enabled by SDN. The related interfaces and protocols in QKD networks enabled by SDN are shown in Section 4. Section 5 presents three useful cases in QKD networks enabled by SDN. Section 6 finally concludes this paper.

2. Progresses in QKD Networks

2.1. *Researches on Architecture of The Networks*

In 2016, Alejandro et al. discussed the impact of SDN on QKD-device deployment, and proposed a quantum sensing SDN architecture by dividing the network into three layers, i.e., application layer, control layer, and infrastructure layer [16]. In 2017, Aguado et al. proposed a distributed NFV MANO architecture by combining NFV orchestration with QKD technology through the scheduling of SDN controller, and integrating IDQ QKD system with experiments [10]. In the same year, as shown in Figure 1a, Yu et al. proposed a three-layer architecture of QKD networks named software-defined QKD network to solve the problem of complex management caused by excessive resource consumption [17]. In addition, as shown in Figure 1b, Zhao et al. proposed a four-layer architecture from the perspective of how to use QKD to enhance the security of SDONs, including application layer, control layer, QKD layer, and data layer [10].

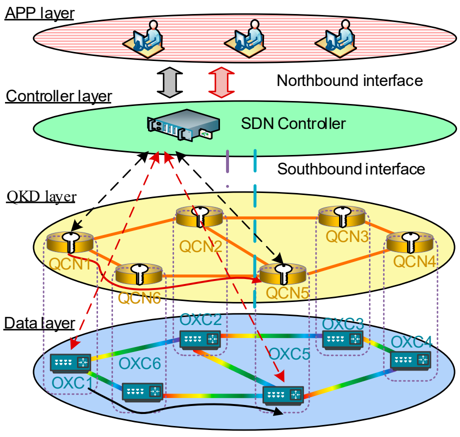

Figure 1. The architecture of optical networks secured by QKD [17].

2.2. Researches on Interfaces and Protocols of the Networks

In terms of protocol extension and interface definition, the following related researches have been conducted around the word. In 2017, as shown in Figure 2, Aguado et al. introduced a new definition of the control layer to provide SSH and HTTPS interfaces to allow NETCONF RPC to be used in SSL/TLS-based solution through SSH, RESTful API and GMPLS protocols [18]. In their other work [19], a node structure for end-to-end QKD services was also proposed, demonstrating the workflow and protocol extensions in different SDN scenarios. In the same year, Dasari et al. proposed a network abstraction model and open table model for software-defined QKD networks [20]. In 2018, Humble et al. used the latest development of OpenFlow protocol in software-defined QKD networks, and realized the control and management of optical networks [21].

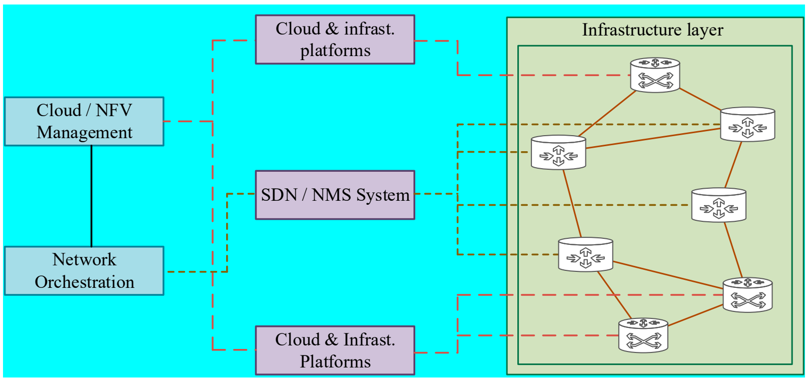

Figure 2. The architecture of QKD networks with cloud/NFV orchestration and SDN control plane [18].

2.3. Experimental Verification of the Networks

In 2017, Chistyakov et al. used a subcarrier quantum system to propose a dynamic quantum routing and secure communication method based on OpenFlow protocol in SDN, further demonstrating the feasibility of applying SDN techniques to QKD networks [22]. In 2018, to effectively alleviate the problem of in-band noise in the QKD network, Ou et al. used machine learning-based approach to estimate physical performances of quantum channel for the successful key generation and transmission [23]. In the same year, Hugues-Salas et al. demonstrated that QKD resources can be successfully allocated through SDN control under DDoS attacks [24]. The results indicate that the application of SDN technology is conducive to alleviate the impact of DDoS attack on QKD networks.

3. Architecture of QKD Network Enabled by SDN

According to the division of functions, the architecture of QKD networks enabled by SDN is introduced in this section. As shown in Figure 3, the architecture of QKD networks enabled by SDN consists of three layers: application layer, control layer, and QKD layer. Users send their requests though northbound interfaces to the controller in control layer, and then controller dynamically controls QKD devices to construct transmission through southbound interfaces. The specific details from the top down are shown below.

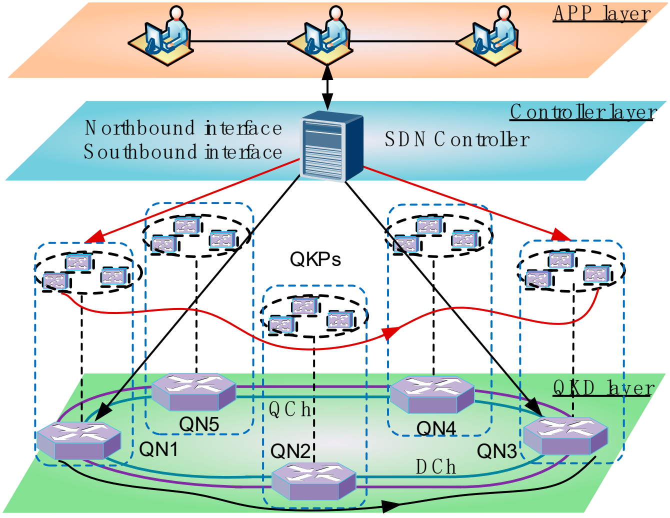

Figure 3. The architecture of QKD network enabled by SDN.

3.1. Application Layer

The application layer is at the top of the architecture of the QKD networks enabled by SDN. It directly faces demands of users and also abstracts network resources for users. Thus, it may meet some requirements such as topological visualization and quality of service from users. Also, the controller can allow the abstraction of network resources like light-path building for QKD and routing for secret-key generation occurring in QKD layer though northbound interfaces. Unlike classical optical networks, the application layer includes two major services, i.e., secret-key provisioning services and security management services. Secret-key provisioning services provide secret keys for the security demands of the networks such as authentication, encryption, and signature. Security management is mainly responsible for the functions such as intrusion detection, virus protection, and security posture sensing, etc.

3.2. Control Layer

Control layer provides a holistic view of QKD networks for the operator. This layer may include one controller or multiple controllers to implement network management over QKD layer and open network capabilities for various applications. Different numbers of controllers in control layer can support hierarchical structure and multiple domains to improve the scalability of the networks. Specifically, application layer receives demands from operators then generates requests and sends them to the controller through its northbound interface. To satisfy the requests as much as possible, the controller calculates and allocates QKD resources with its global network map through the southbound interface. Correspondingly, control layer controls the QKD resources in QKD layer, provides services for multiple applications in application layer, and receives resource allocation and policy information of the key distribution layer.

3.3. QKD Layer

As an additional layer, QKD layer can be implemented as a separate key distribution subsystem. This layer is at the bottom of the architecture concerning with the performances of QKD devices. QKD resources in this layer include WDM links and QKD nodes, which can be used to complete point-to-point QKD and end-to-end QKD respectively. For the QKD nodes, major devices include quantum transmitter (QT), quantum receiver (QR), quantum key pool (QKP) and trust repeater (TR). Among them, QT is used for the preparation of quantum signals according to different QKD protocols such as BB84 protocol. QR is responsible for the detection of quantum signals at receiver ends, and performs quantum state decoding and single-photon detection according to QKD protocol. QKP is used for the storage of secret keys between any two adjacent nodes to satisfy the security demands, and each node has QKP. For the repeaters, there are two types, i.e., quantum repeater [25] and TR [26]. Both of them can be used for secure communication in long distance, since end-to-end secret keys can be relayed by multi-hops point-to-point QKD through quantum repeaters. The former has a better relay ability for quantum signals but it is still in development level, and it is depending on the underlying technologies. The latter has been adopted in actual networks and it can be gradually updated to the former [27]. Thus, TR is generally considered in networking studies. Moreover, process of QKD allows two QKD nodes to exchange secure keys via three types of channels, which are quantum channels (i.e., QC, placed at approximately 1510 nm [28]), measurement-basis channels (i.e., MC, placed at approximately 1530 nm [29]) and data channels (i.e., DC, placed at approximately 1530 nm [29]). These channels can be multiplexed in a fiber by WDM technology [30,31] (e.g., a quantum encryption system can achieve Mb/s key rates with a bandwidth of 200 Gb/s over a 100-km fiber [14]), which imposes a condition that the quantum channel needs to have a guard bandwidth with the other channels of at least 100 GHz. In addition, the interaction of classical information is also required during the above processes according to QKD protocols such as BB84 protocol [32] and two-dimensional distributed phase-reference protocol [33]. Taking BB84 protocol as an example, the processes required by classical information interaction include the comparison of basic measurement and error correction, etc.

4. Interfaces and Protocols in QKD Networks Enabled by SDN

4.1. Related Interfaces

As shown in Figure 4, the main interfaces in controller layer are listed at below.

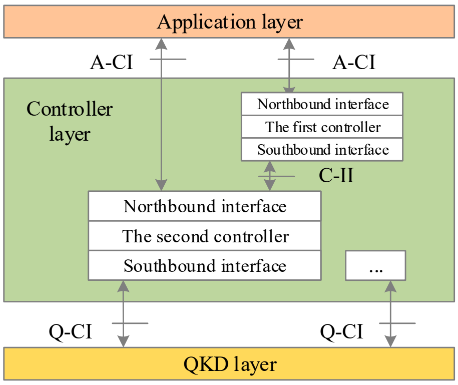

Figure 4. Related interfaces in QKD network enabled by SDN.

(a) QKD Control Interface (Q-CI): It is between the controller and the QKD devices for control and management. The controller can manage QKD resources in QKD layer through this interface to connect with multiple QKD devices.

(b) Controller Interaction Interface (C-II): It is used for the interaction between controllers. Since one controller can provide multiple I-CPI interfaces, allowing simultaneous communication with multiple controllers.

(c) Application Control Interface (A-CI): It serves the interactions from application demands to the controller.

4.2. Southbound Interface Protocol

Southbound interface is used for the management from controller layer to QKD layer to enable some basic control functions like QKD light-path establishment, deletion, and adjustment, etc. Moreover, the types of information should include device configuration, light-path status and network alarm at least. In addition, current SDN version needs to obtain the types of QKD devices, because hybrid connection between different QKD systems will cause failure links to interrupt the generation of secret keys. Considering information came from different devices, this interface should allow multiple protocol selections, and the alternatives are listed as following:

(a) OpenFlow protocol: It can be extended in QKD networks to support resource reporting, link configuration, and other functions of QKD devices.

(b) OpenFlow-Config protocol: It can be used as a supplement for OpenFlow protocol to configure network devices to support OpenFlow. It can use NETconf as the transport protocol.

(c) Traditional management protocols: such as SNMP, TL1, and other protocols.

4.3. Northbound Interface Protocol

Northbound interface is open to the application layer, and its goal is to enable application layer to conveniently modify the underlying QKD resources in QKD layer. The basic control functions of it include topology acquisition, service request, QKD link building, and QKD path calculation, etc. Since application layer needs to provide useful information, the related information model needs to be dealt in controller with physical data uploaded by QKD layer. While adopting more information model will increase the complexity of northbound interface and reduce their interoperability and scalability. General information model can be defined by UML modeling language, and YANG model can be used to construct data model. Moreover, information model is independent of the specific types of interface protocol used in northbound interface. To meet the notification function, the protocol in northbound interface can adopt RESTconf protocol defined by IETF draft-ietf-netconf-restconf-07. As an example, RESTconf protocol will support notification events defined by YANG model, and users can receive the notification by subscribing to the corresponding URL.

5. Three-Use Cases in QKD Networks

Future QKD networks will gradually transform from “point to point” to “multi-point interconnection” to achieve end-to-end secret-key provisioning services, which has a full potential for the application of quantum-secure communication. However, QKD networking for multi-point interconnection needs to meet the characteristics required for a series of networking functions. Thus, there are three issues which need to be addressed: firstly, how to efficiently and flexibly allocate multi-dimensional resources in QKD networks? Secondly, how to construct QKP to complete the dynamic on-demand distribution with limited wavelength resources? Finally, how to guarantee the reliability of QKD networks? The available solutions of these three problems are described below.

5.1. Resource Allocation in the Networks

QKD networks have multi-dimensional resources, including wavelength resources in existing fiber links and secret-key resources in QKPs. During the provisioning of secret-key services, not only secret keys need to be constantly consumed, but also a certain number of wavelength resources need to be occupied. Especially in the case when the number of wavelengths in the network is limited, it is necessary to meet security demands of communication and further improve the wavelength utilization. Thus, how to construct multi-dimensional resources in QKD networks is a necessary problem for the optimization of wavelength utilization. From the perspective of secret-key generation, it is necessary to consider the multi-dimensional resources of optical fiber. In other words, quantum channel and optical channel need to occupy multiple wavelengths, but subject to the entire network’s constraints in terms of wavelength utilization for other services. In addition, the quality of secret-key resources is also affected by global secret-key rates and key pool running time.

In order to solve the above problems, this section establishes a multi-dimensional resource model in QKD networks, designing a strategy for routing and resources allocation of secret-key provisioning services in QKD networks. Since there is a risk that keys will be leaked in the both sides of the communication, secret keys need to be constantly updated to enhance the security. As shown in Figure 5, it shows a specific flowchart for the strategy which mainly includes two steps, i.e., the allocation of secret-key (step 1) and wavelength resources (step 2). For the secret-key allocation, when the requests of services with security demands arrive, the controller will find the corresponding QKP in the nodes given in the requests (step 1.1). The controller randomly selects or first hits a pair of secret keys in the QKP, and sends a secret-key allocation request to the QKP corresponding to the source and destination nodes to inform the station (Step 1.2). If the QKP is empty, this is indicating no resources are available for the allocation and the security requirement of the service will be blocked. Also, for the secret-key update, a certain number of time slices will be allocated for secret-key update periods and the status of QKP will also be updated. For the time-slice allocation, the shortest path from the source to the destination node is calculated based on topology using the shortest path algorithm (step 2.1). Then, allocating time slices based on the first hit algorithm on the calculated path. If time-slice resource is not available, this means that the update will be blocked. Then, the next service will be executed and the status of wavelength occupation in the network will also be updated (step 2.2).

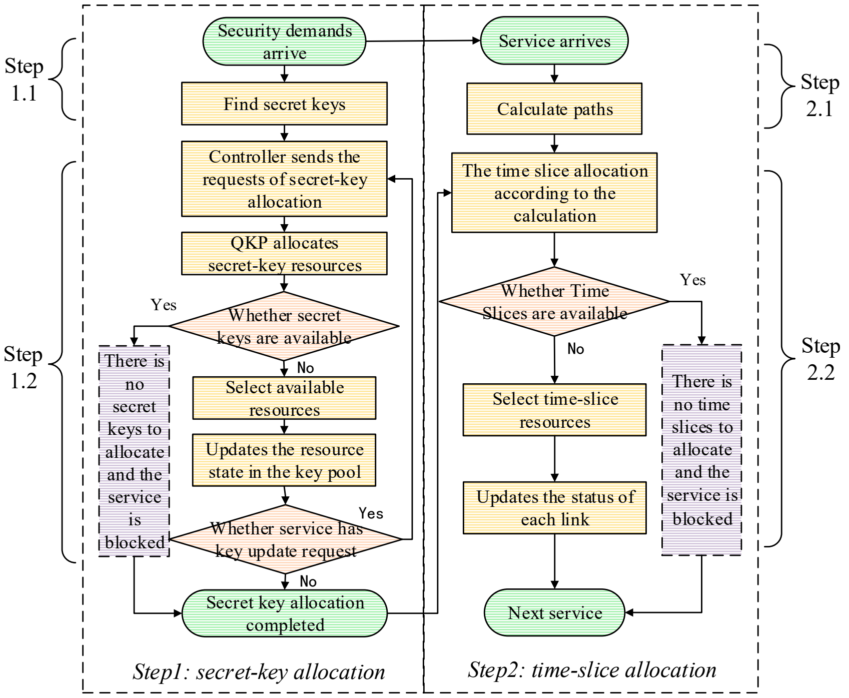
Step 1.1
Security demands arrive
Find secret keys
Controller sends the requests of secret-key allocation
QKP allocates secret-key resources
Whether secret keys are available
Yes
No
Step 1.2
There is no secret keys to allocate and the service is blocked
Select available resources
Updates the resource state in the key pool
Whether service has key update request
Yes
No
Secret key allocation completed
Step1: secret-key allocation
Service arrives
Step 2.1
Calculate paths
The time slice allocation according to the calculation
Whether Time Slices are available
Yes
No
Select time-slice resources
Updates the status of each link
There is no time slices to allocate and the service is blocked
Step 2.2
Next service
Step2: time-slice allocation

Figure 5. The flowchart for routing and resources allocation of secret-key provisioning services.

To verify the feasibility of the proposed strategy, we conducted a simulation with the performances of blocking probability and time-slot utilization under different update periods. As shown in Figure 6a,b, it is obvious that bigger traffic loads will lead higher blocking probability and wavelength utilziation, this is because a limited number of wavelengths can be occuppied. Also, as the update period becomes bigger, the blocking probability and time-slot utilization become lower. More secret keys can be generated by QKD process by occupying more wavelength resources, while bigger secret-key rate developed in the future allows less wavelength occupation and quick secret-key generation.

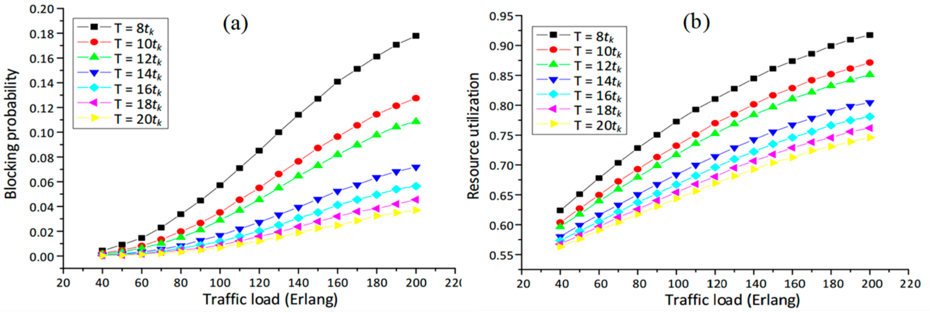

Figure 6. (**a**) The blocking probability, (**b**) the resource utilization.

5.2. Construction of QKP in the Networks

In QKD networks, QKP is a key device used for the storage of secret keys. When security demands arrive, the number of secret keys can be used for the encryption and decryption. However, with the expansion of network scale, user numbers and security requirements, it is necessary to achieve efficient scheduling of wavelength resources and secret-key resources.

To realize efficient generation and consumption of secret-key resources, a construction of QKP in QKD network is proposed in this section. QKP here represents a device abstracted by each pair of nodes for storing the secret keys generated between them. As shown in Figure 7, Dch and Qch represent channels used for the transmission of optical signals and quantum signals based on QKD process, respectively. OTDM technology can be used here to divide transmission channels into various time slices. During each time slot, a certain number of secret keys can be generated and stored in QKP by designing a routing path and allocating time slices. Thus, a routing, wavelength, and key assignment (RWKA) algorithm is designed for allocating available time slots to generate secret keys to fill QKPs. The RWKA algorithm is divided into three steps, i.e., calculating routes and assigning wavelengths for secret-key provisioning services through Dchs and Qchs. First, the k-short path algorithm is used to select short route, and then, first fit (FF) algorithm is used for wavelength allocation to occupy available wavelengths for key distribution. Besides, please note that secret keys in QKPs are stored in bits and cannot be reused for another encryption.

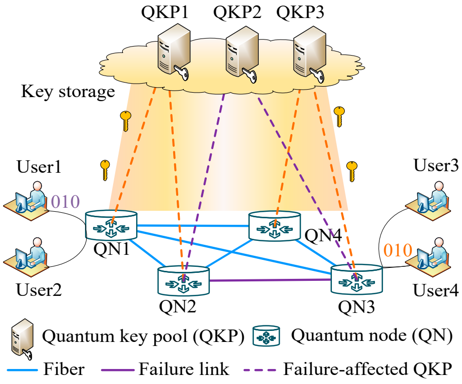

Figure 7. The QKD network architecture with QKP.

We evaluated simulation performances of RWKA algorithm in QKD networks with NSFnet topology (i.e., 14 nodes and 21 links). Compared with uniform (case 1) and non-uniform (case 2) time-slot allocation, the blocking probability and time-slice utilization of secret-key provisioning service are shown in Figure 8a,b. It is clear to see that blocking probability and resource utilization of secret-key provisioning services gradually increases with bigger traffic load. This is because the wavelength resources in each single fiber are limited and the wavelength channels need to carry a large number of services. The simulation evaluated the security probability of the control channel and the security probability of the data channel respectively, and the results were shown to verify the efficiency of the solution. In addition, the size of QKP can be further studied to match the secret-key rate of QKD system and security demands in a real situation.

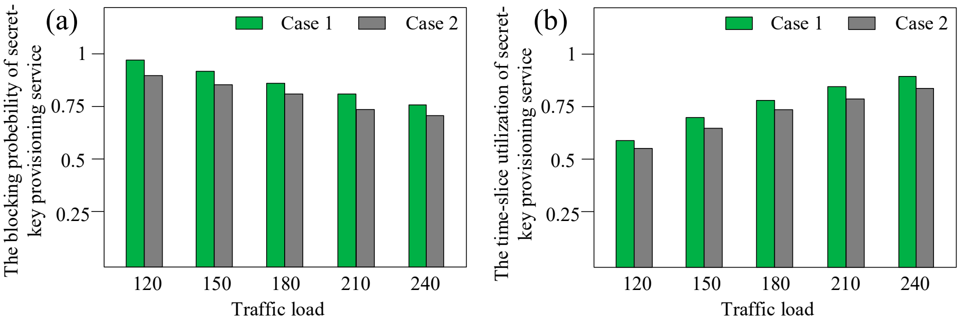

Figure 8. (**a**) The ratio of successful QKP construction, (**b**) the resource utilization.

5.3. *Survivability of the Networks*

Similar to classical optical networks, the survivability of QKD networks is attracting more and more attention. The secret-key provisioning services in QKD networks can normally satisfy the security demands of users. As an inevitable problem, a single link failure will interrupt the services in failure-affected links, indirectly causing a large amount of capacity. Therefore, how to protect secret-key provisioning services in QKD networks is an important problem. This section provides two protection schemes (i.e., secret-key dedicated protection and shared protection) against quantum network failures. As shown in Figure 9, secret-key dedicated protection can allocate dedicated wavelengths in different working and protection paths for each service, and then performs QKD on two different paths simultaneously. When a link failure occurred in the working path, QKD can also be processed on the protection path to generate secret keys. Compared with the dedicated protection, secret-key shared protection can improve resource utilization by sharing the protection resources among several services. When link failures occur in the network, secret-key provisioning services can be protected by using extra pre-provisioned network resources.

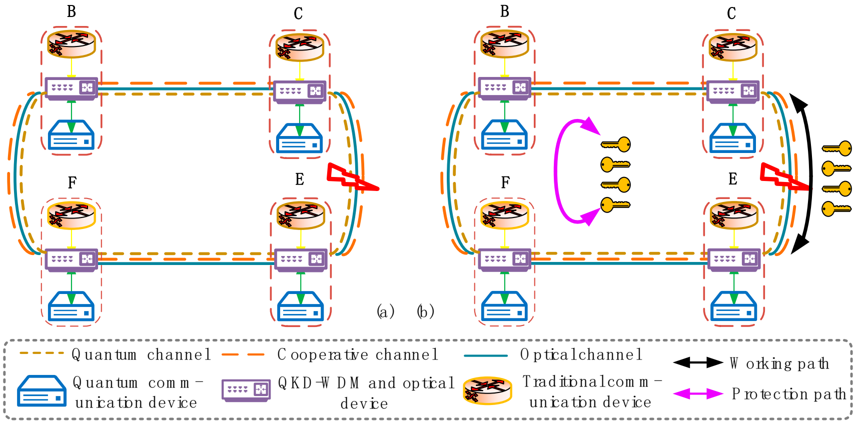

Figure 9. The protection in QKD networks, (**a**) a link failure occurred in the network, (**b**) the protection in the network.

To achieve the protection, there are three sub-problems that need to be considered in the protection schemes. Specifically, the first sub-problem is that links in working path and protection path may face same type of failure risks, since the secret-key provisioning services are transmitted in a general topology. Moreover, the calculation of working path and protection with different failure risk will accumulate a large number of limitations about failure risks; thus, the second sub-problem is high blocking probability caused by the limitations. In addition, different secret-key rates in different links are changing over time, so how to generate secret keys in a path to meet security demands is the third sub-problem. Based on the above sub-problems, this paper proposes two protection schemes of secret-key provisioning services, and their working and protection resources are calculated by RWKA. First, a dedicated protection algorithm is proposed, which allocates working and protecting resources for the services. Second, to make full use of resources, we designed a shared protection algorithm to share protection resources among several services.

To verify the effectiveness, we conducted a simulation of the two proposed protection schemes in terms of blocking probability, resource utilization, and secret-key consumption. As shown in Figure 10a–c, results show that the adaptive shared protection algorithm reduces the blocking probability of the dedicated protection. This is because a smaller key update cycle will increase the blocking probability, which can be reduced by increasing the maximum sharing threshold, as shown in the results. Therefore, there is a trade-off between survivability and security. In addition, these results also proved that our proposed algorithm is an effective way to provide the protection, while this process will accelerate secret-key generation.

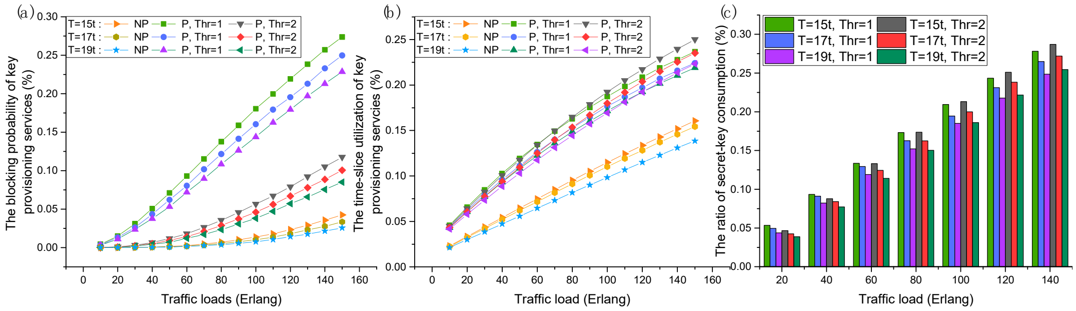

Figure 10. (**a**) The blocking probability, (**b**) the resource utilization, (**c**) the ratio of secret-key consumption.

6. Conclusions

SDN is a technology that separates the control and management of the networks from the data transmission and forwarding functionalities. It is also a promising idea to be applied in QKD networks for convenient optimization of the interaction of devices, resources and operations. This paper systematically introduces the QKD networks enabled by SDN, which logically controls QKD resources and abstract them to the application layer through northbound and southbound interfaces and related protocols, to finally realize a flexible and intelligent QKD networks. Moreover, three-use cases, including multi-resources allocation, secret-key management, and survivability guarantee, are provided as paradigms worthy of study. We described the process of the three-use cases, and numerous simulation results show the effectiveness of them. However, the compatibility of QKD networks and traditional optical networks is a current major challenge, and high costs will arise due to the redeployment of QKD networks. Also, more interesting related issues will be researched in the future.

Author Contributions: The writing of the draft was by H.W., the review, editing of the draft were responsible by Y.Z., and the language improvement of the draft was by A.N.

Funding: This research was funded by China State Grid Corp Science and Technology Project, 5210ED180047; National Natural Science Foundation of China (NSFC), 61822105, 61571058, 61601052; BUPT Excellent Ph.D. Students Foundation, CX2019215.

Conflicts of Interest: No conflict of interest.

References

1. Paul, A.M.D. *The Principles of Quantum Mechanics*, 3rd ed.; Clarendon Press: Oxford, UK, 1947.

2. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2014**, *8*, 595–604. [CrossRef]
3. Wang, W.; Zhao, Y.L.; Yu, X.S.; Chen, B.W.; Zhang, J. Resilient Fiber-based Quantum Key Distribution (QKD) Networks with Secret-key Re-allocation Strategy. In Proceedings of the OFC, San Diego, CA, USA, 3–7 March 2019.
4. Islam, N.T.; Lim, C.C.W.; Cahall, C.; Kim, J.; Gauthier, D.J. Provably secure and high-rate quantum key distribution with time-bin qudits. *Sci. Adv.* **2017**, *3*, 1–6. [CrossRef]
5. Beatrice, D.L.; Davide, B.; Daniele, C.; Yunhong, D.; Kjeld, D.; Karsten, R.; Leif, O. Experimental demonstration of the DPTS QKD protocol over a 170 km fiber link. *Appl. Phys. Lett.* **2019**, *114*. [CrossRef]
6. Mercian, A.; Mcgarry, M.P.; Reisslein, M.; Kellerer, W. Software defined optical networks (SDONs): A Comprehensive Survey. *IEEE Commun. Surv. Tuts* **2016**, *18*, 2738–2786.
7. Partha, B.; Zhang, S.Q.; Pulak, C.; Sang-Soo, L.; Jong, H.L.; Biswanath, M. Software-defined optical networks (SDONs): A survey. *Photonic Netw. Commun.* **2014**, *28*, 4–18.
8. Cao, Y.; Zhao, Y.L.; Yu, X.S.; Cheng, L.J.; Li, Z.Q.; Liu, G.J.; Zhang, J. Experimental Demonstration of End-to-End Key on Demand Service Provisioning over Quantum Key Distribution Networks with Software Defined Networking. In Proceedings of the OFC, San Diego, CA, USA, 3–7 March 2019.
9. Cao, Y.; Zhao, Y.L.; Colman-Meixner, C.; Yu, X.S.; 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]
10. Zhao, Y.L.; Cao, Y.; Wang, W.; Wang, H.; Yu, X.S.; Zhang, J.; Massimo, T.; Wu, Y.; Biswanath, M. Resource allocation in optical networks secured by quantum key distribution. *IEEE Commun. Mag.* **2018**, *56*, 130–137. [CrossRef]
11. Cao, Y.; Zhao, Y.L.; Yu, X.S.; Wu, Y. Resource assignment strategy in optical networks integrated with quantum key distribution. *J. Opt. Commun. Netw.* **2017**, *9*, 995–1004. [CrossRef]
12. Cao, Y.; Zhao, Y.L.; Li, J.; Lin, R.; Chen, J.J. Reinforcement Learning Based Multi-Tenant Secret-Key Assignment for Quantum Key Distribution Networks. In Proceedings of the OFC, San Diego, CA, USA, 3–7 March 2019.
13. Wang, H.; Zhao, Y.L.; Yu, X.S.; Ma, Z.Z.; Wang, J.Q.; Avishek, N.; Yi, L.T.; Zhang, J. Protection Schemes for Key Services in Optical Networks Secured by Quantum Key Distribution (QKD). *J. Opt. Commun. Netw.* **2018**, *3*, 67–78. [CrossRef]
14. Cao, Y.; Zhao, Y.L.; Wu, Y.; Yu, X.S.; Zhang, J. Time-scheduled quantum key distribution (QKD) over WDM networks. *J. Lightwave Technol.* **2018**, *36*, 3382–3395. [CrossRef]
15. Alejandro, A.; Emilio, H.-S.; Paul, A.H.; Jaume, M.; Alasdair, B.P.; Philip, S.; Jake, E.K.; Chris, E.; John, G.R.; Mark, G.T.; et al. Secure NFV Orchestration Over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources. *J. Lightwave Technol.* **2017**, *35*, 1357–1362.
16. Aguado, M.A.; Martín, A.V.; López, D.R.; Peev, M.; Martínez, M.J.; Rosales, B.J.L.; Iglesia, F.; Gómez, M.; Hugues, S.E.; Lord, A.; et al. Quantum-Aware Software Defined Networks. In Proceedings of the QCrypt 2016, Washington, DC, USA, 12–16 September 2016.
17. Yu, W.; Zhao, B.; Yan, Z. Software defined quantum key distribution network. In Proceedings of the ICCC, Chengdu, China, 13–16 December 2017.
18. Alejandro, A.; Victor, L.; Jesus, M.-M.; Momtchil, P.; Diego, L.; Vicente, M. Hybrid conventional and quantum security for software defined and virtualized networks. *IEEE/OSA J. Opt. Commun. Netw.* **2017**, *9*, 819–825.
19. Alejandro, A.; Victor, L.; Jesus, M.-M.; Momtchil, P.; Diego, L.; Vicente, M. Virtual network function deployment and service automation to provide end-to-end quantum encryption. *IEEE/OSA J. Opt. Commun. Netw.* **2018**, *10*, 421–430.
20. Dasari, V.R.; Sadlier, R.J.; Geerhart, B.E.; Snow, N.A.; Williams, B.P.; Humble, T.S. Software-defined network abstractions and configuration interfaces for building programmable quantum networks. In Proceedings of the SPIE 10212, Advanced Photon Counting Techniques XI, Anaheim, CA, USA, 5 May 2017; p. 102120U.
21. Travis, S.H.; Ronald, J.S.; Brian, P.W.; Ryan, C.P. Software-defined quantum network switching. In Proceedings of the SPIE 10652, Disruptive Technologies in Information Sciences, Orlando, FL, USA, 9 May 2018; p. 106520B.
22. Chistyakov, V.V.; Sadov Oleg, L.; Vasiliev, A.B.; Egorov, V.I.; Kompaniets, M.V.; Fedchenkov, P.V.; Lazo, O.I.; Shevel, A.E.; Buldakov, N.V.; Gleim, A.V.; et al. Software-defined subcarrier wave quantum networking operated by OpenFlow protocol. *arXiv* **2017**, arXiv:arXiv170909081C.

23. Ou, Y.; Hugues-Salas, E.; Ntavou, F.; Wang, R.; Bi, Y.; Yan, S.Y.; Kanellos, G.; Nejabati, R.; Simeonidou, D. Field-Trial of Machine Learning-Assisted Quantum Key Distribution (QKD) Networking with SDN. In Proceedings of the ECOC 2018, Roma, Italy, 23–27 September 2018.
24. Hugues-Salas, E.; Ntavou, F.; Ou, Y.; Kennard, J.E.; White, C.; Gkounis, D.; Nikolovgenis, K.; Kanellos, G.; Erven, C.; Lord, A.; et al. Experimental Demonstration of DDoS Mitigation over a Quantum Key Distribution (QKD) Network Using Software Defined Networking (SDN). In Proceedings of the OFC 2018, San Diego, CA, USA, 11–15 March 2018.
25. Varnava, C.; Stevenson, R.M.; Nilsson, J.; Skiba-Szymanska, J.; Dzurňák, B.; Lucamarini, M.; Penty, R.V.; Farrer, I.; Ritchie, D.A.; Shields, A.J. An entangled-LED-driven quantum relay over 1km. *NPJ Quantum Inform.* **2016**, *2*, 16006. [CrossRef]
26. Stacey, W.; Annabestani, R.; Xiongfeng, M.; Lütkenhaus, N. The Security of Quantum Key Distribution using a Simplified Trusted Relay. *Phys. Rev. A* **2014**, *91*, 1–11. [CrossRef]
27. Stephanie, W.; David, E.; Ronald, H. Quantum internet: A vision for the road ahead. *Science* **2019**, *362*, 1–9.
28. McCormick, C.F.; Marino, A.M.; Boyer, V.; Lett, P.D. Strong low-frequency quantum correlations from a four-wave-mixing amplifier. *Phys. Rev. A* **2008**, *78*, 043816. [CrossRef]
29. Boris, K.; Charles, C.W.L.; Raphael, H.; Nicolas, G.; Ming, J.L.; Daniel, N.; Bruno, S.; Rob, T.; Hugo, Z. Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre. *Nat. Photon.* **2015**, *9*, 163–168.
30. Beatrice, D.L.; Davide, B.; Daniele, C.; Francesco, D.R. Record-High Secret Key Rate for Joint Classical and Quantum Transmission Over a 37-Core Fiber. In Proceedings of the IPC, Hilton Palacio del Rio, San Antonio, TX, USA, 4–7 December 2018.
31. Ken-ichiro, Y.; Mikio, F.; Akihiro, T.; Seigo, T.; Yoshihiro, N.; Akihisa, T.; Shigehito, M.; Taro, Y.; Zhen, W.; Masahide, S.; et al. High-speed wavelength-division multiplexing quantum key distribution system. *Opt. Lett.* **2012**, *37*, 223–225.
32. Charles, H.B.; Gilles, B. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference Computers, Systems, and Signal Processing, Bangalore, India, 9–12 December 1984.
33. Davide, B.; Jesper, B.C.; Mario, A.U.C.; Yunhong, D.; Søren, F.; Karsten, R.; Leif, K.O. Two-dimensional distributed-phase-reference protocol for quantum key distribution. *Sci. Rep.* **2016**, *6*, 36756.

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).