IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 9, 2019, accepted April 30, 2019, date of publication May 7, 2019, date of current version May 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2915378

Resilient Quantum Key Distribution (QKD)-Integrated Optical Networks With Secret-Key Recovery Strategy

HUA WANG[1], YONGLI ZHAO[1], (Senior Member, IEEE), XIAOSONG YU[1], AVISHEK NAG[2], (Senior Member, IEEE), ZHANGCHAO MA[3], JIANQUAN WANG[3], LONGCHUAN YAN[4], AND JIE ZHANG[1]

[1]State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]School of Electrical and Electronic Engineering, University College Dublin, Dublin 4, 999015 Ireland
[3]Chinese Academy of Sciences Quantum Network Co., Ltd., Shanghai 201315, China
[4]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100000, China

Corresponding author: Yongli Zhao (yonglizhao@bupt.edu.cn)

This work was supported in part by the Optical Fiber Communication Conference and Exhibition, under Grant OFC/NFOEC 2019, W2A.25, in part by the National Science and Technology Major Project under Grant2017ZX03001016, in part by the National Natural Science Foundation of China (NSFC) under Grant 61822105, Grant 61571058, and Grant 61601052, in part by the BUPT Excellent Ph.D. Students Foundation under Grant CX2019215, and in part by the State Key Laboratory of Advanced Optical Communication Systems Networks of China.

ABSTRACT Quantum key distribution (QKD) promises to deliver secure keys, which can be applied for security demands in optical networks by using cost-efficient and scalable lightpaths. To achieve such secure communication, the QKD integrated with optical networks has become a promising scenario to provide key provisioning services in optical networks. As an inevitable problem, the occurrence of failures becomes a challenge for the resiliency of the network. In that context, this paper studies the resilient QKD-integrated optical networks against single link failure. By analyzing and quantifying the key provisioning services, we constructed the secret-key flow model (SKFM) for the failure-affected and failure-unaffected cases. Based on the SKFM, a secret-key recovery strategy (SKRS) including three algorithms (i.e., one-path recovery method (OPRM), multi-path recovery method (MPRM), and time window-based recovery method (TWRM)) is designed to recover failure-affected key provisioning services in the network. The simulation work has been conducted to evaluate the performance of OPRM, MPRM, and TWRM in terms of key-service recovery ratio, secret-key recovery ratio, wavelength consumption ratio, and secret-key consumption ratio. Numerical results show that the three algorithms can recover failure-affected key provisioning services effectively, i.e., the MPRM outperforms the OPRM and the TWRM outperforms the MPRM. Better recovery can be realized by sacrificing more wavelength and secret-key resources, which are also required for the delivery of the QKD in the network. Thus, a trade-off can be achieved between the recovery of key provisioning services and the delivery of the QKD on wavelength resources and secret-key resources.

INDEX TERMS Optical networks, security, quantum key distribution (QKD), resilient, recovery.

I. INTRODUCTION

Most of the high-bandwidth information carried by the optical networks is generated because of the increasing demands of the users [1]. With diversifying types of users' demands, the security of information in the optical networks has always been regarded as a serious problem [2], [3]. The use of traditional encryption methods and systems based on mathematical complexity are restricted as they are effective only if the emerging quantum computer can be used [4]. Recently, a promising technology, quantum key distribution (QKD), can provide proven secure keys to enhance the security of information based on the physical properties of the quantum mechanism [5]–[7]. It has been proposed and

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Arshad.

experimentally integrated into optical networks mainly by wavelength division multiplexing (WDM) [8]–[11]. Moreover, the technology on quantum-classical signal coexistence in one fiber has been continually developed to distribute secret keys, and existing optical networks can offer necessary wavelength resources for the widespread adoption of QKD in commercial perspective. Therefore, QKD can offer guaranteed security of data in optical networks, which promises to become a mainstream trend for secure optical networks in the future.

Nowadays, many studies contribute to QKD-integrated optical networks mainly focusing on the physical layer and network layer. For instance, quantum channel multiplexed with classical channels in a fiber continues to make breakthroughs in distance [12]–[15], secret-key management like quantum key pool (QKP) is constructed to alleviate the low secret-key rate of current QKD systems [16], and several syncretic architectures proposed for the integration of QKD aim for the transport of QKD in optical networks [17]–[19]. Based on these, wavelength resources in optical networks can be effectively assigned for QKD [17], [18], [20], secret-key provision proposed in several methods can satisfy security demands in QKD networks and QKD-integrated optical networks [16], [21] and [22]. However, secret-key provision requires a quality of delivery guarantees in QKD-integrated optical networks. As an inevitable problem, the occurrence of failures in the network will have a great influence on them. For example, a single link failure will disrupt the secret-key distribution on a link and affect the key generation on some corresponding routes. Such interruption intuitively violates users' demands on security, and further results in a bigger artificial recovery time and higher capital expenditure indirectly. Different from traditional survivability, a link failure in such network will cause an interruption of secret-key generation, which means the secret keys in failure-affected QKPs will be consumed until it is hard to satisfy security demands. Thus, recovery of key provisioning services for the security demands in failure-affected QKD networks is an important problem. Recent efforts made for practical networks provide operators with several delivery methods of QKD, and nowadays the resiliency of the network attracts more and more attention [23].

This paper focuses on strengthening the resiliency of QKD-integrated optical networks against a single link failure. The object is to recover secret-key provision (referred to key provisioning service hereafter) in failure-affected QKPs as much as possible. In order to achieve the object, the following three main contributions have been completed. 1) We analyzed and quantified the key-provisioning services and their failure-affected cases in the network. 2) We constructed the network model and secret-key flow model (SKFM) including the relationship between secret-key generation and consumption to simplify the problem. 3) Based on the quantified services, failure-affected cases and SKFM, we propose a secret-key recovery strategy (i.e., SKRS) including three secret-key recovery algorithms, i.e., one-path recovery method (OPRM), multi-path recovery method (MPRM), and time window-based recovery method (TWRM). These algorithms are designed to solve the problem, and they are capable of recovering failure-affected key provisioning services as much as possible. To verify it, OPRM, MPRM, and TWRM are simulated to evaluate the feasibility of SKRS in terms of successful recovery ratio, secret-key recovery degree, wavelength consumption ratio, and secret-key consumption ratio. Numerical simulation results show that three methods can recover failure-affected key provisioning services in different degrees. Results also illustrate that more wavelength and secret-key resources are used for the recovery thereby leaving fewer resources for the delivery of QKD and security demands. Thus, a trade-off exists between the recovery of key provisioning services and the delivery of QKD.

The rest of this paper is organized as follows. Section 2 introduces some feasible technologies to form the architecture of QKD-integrated optical networks. The description of three parameters, the analysis of the secret-key flow of QKPs, and the construction of SKFM are given in Section 3. Section 4 designs an SKRS including three algorithms (i.e., OPRM, PMRM, and TWRM) for the recovery of key provisioning services according to SKFM. We simulate the algorithms and present numerical results to evaluate the validity in Section 5. Finally, the paper is summarized in Section 6.

II. QKD-INTEGRATED OPTICAL NETWORKS

This section presents a detailed introduction to the QKD-integrated optical networks. For the sake of clarity, the aspects of communication secured by QKD and QKP in secret-key delivery are described before the architecture of the networks.

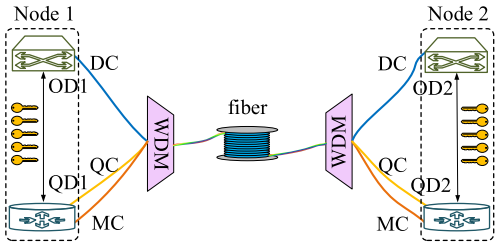

FIGURE 1. QKD process between two nodes.

A. COMMUNICATIONS SECURED BY QKD

QKD can secure point-to-point communication as shown in Fig. 1. Each pair of nodes in the network physically includes quantum devices (QDs) and optical devices (ODs) to perform QKD. Also, the construction of channels used for QKD (i.e., quantum channels (QCs) and measurement-based channels (MCs)) and data channels (DCs) used for data services can save costs by using WDM in one fiber [8]–[11]. Thus, each pair of link-connected nodes can share common secret keys to secure data services by QKD. Ideally, when a confidential communication was required between node 1 and

node 2, two QDs generate secret keys by QKD for the service between two nodes. In addition, when it comes to different quantum protocols, the secret keys generated by QKD can be performed through different processes.

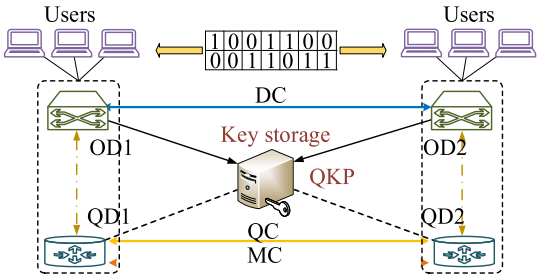

FIGURE 2. QKP in secret-key delivery.

B. QKP IN SECRET-KEY DELIVERY

To alleviate low secret-key rate that was illustrated in several experimental works [8]–[10], QKP has been proposed for the secret-key management such as secret-key storage between two nodes [16], [17]. As shown in Fig. 2, QKPs are configured between each pair of adjacent nodes. Each pair of nodes can continually generate secret keys by performing QKD and then store the keys in QKPs. When the services with security demand arrive, secret keys in QKPs are extracted to these services as needed [16], and the encrypted services can be transmitted to the other node.

C. THE ARCHITECTURE OF QKD-INTEGRATED OPTICAL NETWORKS

The architecture of QKD-integrated optical networks is illustrated in Fig. 3(a). Point-to-point QKD can secure the communication between any pairs of adjacent nodes, QKP can store the keys for the large security demands, and thus a long-distance secure communication can be offered by the networks. The architecture of the networks includes QKD layer and optical layer to separate QKD function from traditional optical communication. QKD layer is responsible for the secret-key distribution, and optical layer can transmit encrypted information by traditional infrastructure. They respectively consist of QDs and ODs, which are co-located in a common physical node. To perform resources allocation for QKD, QDs require some components including QKD transceiver, repeater, and QKD server, etc. At the same time, multiple QDs can be configured in a node to communicate with multiple nodes simultaneously in parallel mode [24]. To make different devices in a uniform manner, the common protocols [25], [26] can be used for the different characteristics and interfaces of devices [27], [28]. Among QKD devices, quantum repeater [29], [30] or trusted repeater [31] is critical to realize long-distance secure communication. The former has a better relay ability for quantum signals but it is still in the development stages, which is depending on the underlying technologies. The latter on the other hand, has been adopted in actual networks and it can be gradually

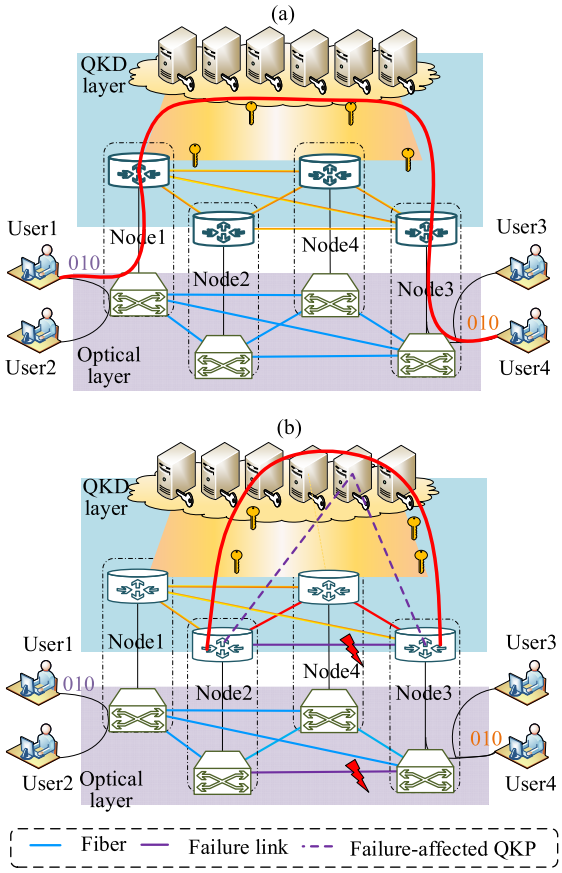

FIGURE 3. QKD-integrated optical networks, (a) the architecture of QKD-integrated optical networks, and (b) QKD-integrated optical networks with a link failure.

updated to a quantum repeater [32]. Thus, trusted repeater is considered in this paper. As an example of a failure-affected network shown in Fig. 3(b), when a link failure occurs between node 2 and node 3, the delivery of QKD in this link will be interrupted, and the QKP 5 used for node 2 and node 3 will also be interrupted to get secret keys. To solve this problem, the secret keys in QKP 5 can be jointly recovered by other QKPs to satisfy the security demands between node 2 and node 3, which is described in section 4 in detail.

III. SECRET-KEY FLOW MODEL (SKFM) IN QKD-INTEGRATED NETWORKS

The secret-key flow model (SKFM) is used for the mathematical description of secret keys in QKP. It can offer a simplified secret-key flow from dynamic to static and allow a secret-key recovery strategy designed for the problem. Thus, the key provisioning services is first illustrated, and then the formulation of secret-key flow is constructed step by step.

A. KEY PROVISIONING SERVICE

Depending on quantum protocols like BB84 [33], point-to-point QKD can distribute secret keys between each pair of adjacent nodes in the network [32], [34]. For the security demands of end-to-end secret-key demands, several factors

including QKD-limited distance, etc., need to be considered in the network. As we know, the distance of QKD is limited, and practical optical networks exist in both short and long links. For the short links, point-to-point QKD can be directly performed in a short link or several short links, as long as their total distance meets the distance limit of QKD [18]. For the long links, multi-hop point-to-point QKD on several short links can distribute secret keys by repeaters [35], [36]. However, it has the disadvantage of consuming extra time that will affect the quality of services (i.e., a few minutes are required for synchronization and stabilization time in a QKD systems). Since point-to-point secret keys (PSK) can be generated by QKD and stored in QKP, end-to-end secret keys (ESK) can also be generated by multi-hop point-to-point QKD but these ESKs are needed to be stored in the QKP too so that security demands can access them quickly. But it comes at the cost of extra wavelength consumption for the process of QKD relay. Hence, we suppose the QKPs with ESK exist between parts of node pairs with huge security demands. The main advantage of this approach is that it allows quick key provisioning services for the huge security demands via the storage of end-to-end secret keys. Accordingly, three cases of secret-key delivery are shown in Fig. 4–6 considering the distance limitations of QKD.

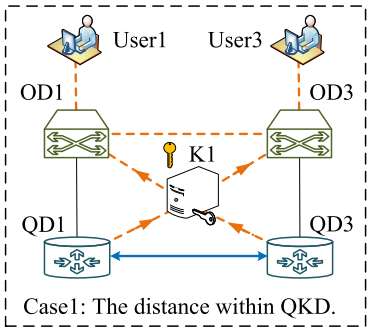

FIGURE 4. Case 1 of the secret-key delivery in QKD-integrated networks.

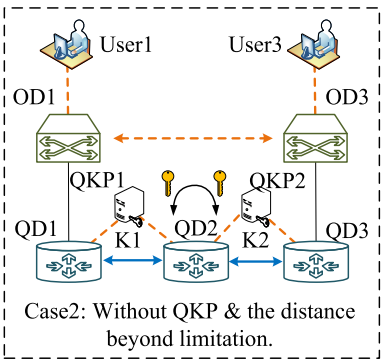

FIGURE 5. Case 2 of the secret-key delivery in the QKD-integrated networks.

a) In the case 1, if the distance of node pair QD1 and QD3 is within the limitation distance, then PSK K1 can be generated by QKD in the QKP between QD1 and QD3, and two users can directly use K1 in the QKP between QD1 and QD3.

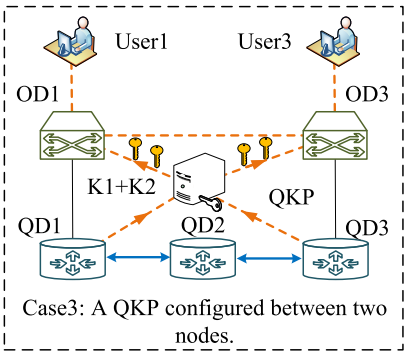

FIGURE 6. Case 3 of the secret-key delivery in the QKD-integrated networks.

b) In the case 2, if the distance is beyond the limit distance of QKD and security demands in the node pairs are not large, the services between QD1 and QD3 can be first encrypted and decrypted by K1 in QKP1 and then encrypted and decrypted by K2 in QKP2 through a trusted repeater.

c) In the case 3, if the distance between a node pair is beyond the limit distance of QKD and security demands in the node pairs are large, different from case 2, the QKP with ESK storage is configured between QD1 and QD3 by the secret keys K1 + K2 [20]. Thus, multi-hop point-to-point QKD between QD1 and QD3 can store ESK in QKP in advance, and two users can directly use the secret keys in QKP between QD1 and QD3. Examples of the specific generation of PSK and ESK are given as follows. When a security demand arrives between user 1 and user 3, point-to-point QKD can be performed between QD1 and QD2, QD2 and QD3, respectively, and the generated PSK can be used for the generation of ESK between QD1 and QD3.

B. NETWORK MODELING

The QKD-integrated optical network is represented as $G = (V, L, W, P, P')$, where $V = \{v_1, \cdots, v_n\}$ and $L = \{l_1, \cdots, l_n\}$ respectively denote the nodes and links in the network.$W = \{w_1, \cdots, w_n\}$ is the set of wavelength resources used for QKD in a bi-directional fiber. $P = \{p_1, \cdots, p_n\}$ and $P' = \{p'_1, \cdots, p'_n\}$ respectively indicate that each QKP has only PSK or still contains ESK. Whether it is QKP with PSK or also with ESK, the secret keys stored in it were generated by QKD and then used for the security demands. Thus, three parameters are defined in QKP corresponding to the secret-key generation and consumption: secret-key generation rate (R_{kg}), secret-key consumption rate (R_{kc}), and existing secret-key amount (K_e). Since R_{kc} comes from security demands and changes with time, the value of R_{kc} is different. When $R_{kg} - R_{kc} \geq 0$, surplus secret keys can be stored in QKP as K_e. When $R_{kg} - R_{kc} < 0$, K_e in QKP can be used to satisfy R_{kc}. Therefore, secret keys in QKP can always meet security demands when the network works normally.

If a link failure occurs in the network, it will break the balance of secret-key generation-consumption relationship in

QKPs, especially for the secret-key generation in the failure-affected link and some corresponding ESK. Specifically, depending on whether a QKP is configured before or after a link failure, the relationship may be divided into three states, i.e., supply exceeds demand (SED), demand exceeds supply (DES), and failure occurred (FO). Before the failure occurs, R_{kc} in QKP can mainly be supported by K_e no matter $R_{kg} - R_{kc} \geq 0$ (i.e., SED) or $R_{kg} - R_{kc} < 0$ (DES), that is, K_e in QKP at least should be greater than 0. After the fault occurs, the R_{kg} of failure-affected QKP turns into 0 directly, and the K_e can be used for the R_{kc} until it is reduced to 0, while the K_e in the QKP cannot support the consumption for a long time (i.e., FO). In order to conveniently represent the impact of a link failure on QKP, we present the above states in Fig. 7. As the instance shown in the figure, a link connecting QD 1 and 2 in the network suffers a fiber cut. The secret-key generation that was originally distributed between the two nodes is interrupted. When there is a security demand from node 1 to 2, it cannot always be satisfied since the K_e of QKP will be consumed to 0.

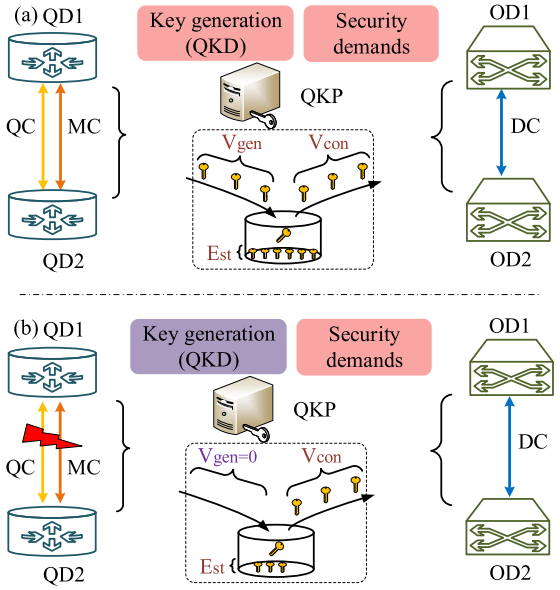

FIGURE 7. (a) Secret keys in QKP, (b) a link failure occurred in QKD-integrated optical network.

C. SECRET-KEY FLOW MODELING

Based on the above analysis of the secret-key generation-consumption relationship for a QKP, we model the secret-key flow in QKP at some time points (i.e., $t+1$, $t+2$, and $t+T$) and in a time period (i.e., T), respectively. Then, we construct the secret-key flows in SED, DES, and FO states. Finally, all the secret-key flows of QKPs in the network are expressed in the form of secret-key volume matrix. The specific symbol notation is given in Table 1.

The secret-key flow of SK-QKD and RTKG at time t and during time period T are shown in equations (1) – (4). The size of v_{gen} and v_{con} are important for K_{ij} and changes in either of them will affect the value of K_{ij}. Without losing generality, v_{gen} and v_{con} can be taken from the average value of secret-key generation and consumption rates within a Δt. Thus, the $v_{gen} - v_{con}$ secret keys can be stored in QKP in each Δt, and $\sum_{1\cdots T}\left(\left(v_{gen} - v_{con}\right) * \Delta t\right)$ secret keys can be stored during a T consisting of several time units.

TABLE 1. Parameters.

Notation	Definition
Δt:	Time unit.
t:	Time point.
T:	Time period.
v_{gen}:	Secret-key generation rate per time unit.
v_{con}:	Secret-key consumption rate per time unit.
K_{ij}^{0}:	The initial secret-key volume between node i and j.
K_{ij}^{t}:	The secret-key amount at time t between node i and j.
K_{ij}^{t+1}:	The secret-key amount at time $t+1$ between node i and j.
K_{ij}^{t+2}:	The secret-key amount at time $t+2$ between node i and j.
K_{ij}^{T}:	The secret-key amount at time T between node i and j.
K_{ij}^{t+T}:	The secret-key amount during T between node i and j.

- The secret-key flow in QKP at time $t+1$:

$$K_{ij}^{t+1} = K_{ij}^{t} + \left(v_{gen} - v_{con}\right) * \Delta t \tag{1}$$

- The secret-key flow in QKP at time $t+2$:

$$K_{ij}^{t+2} = K_{ij}^{t+1} + \left(v_{gen} - v_{con}\right) * \Delta t \tag{2}$$

- The secret-key flow in QKP at T:

$$K_{ij}^{T} = K_{ij}^{t+T-1} + \left(v_{gen} - v_{con}\right) * \Delta t \tag{3}$$

- The secret-key flow in QKP during T period:

$$K_{ij}^{t+T} = K_{ij}^{\mathrm{t}} + \sum_{1\cdots T}\left(\left(v_{gen} - v_{con}\right) * \Delta t\right) \tag{4}$$

In addition, three states i.e., SED, DES, and FO are shown in equations (5) - (7) existed with a trade-off between v_{gen} and v_{con} on K_e.

- SED:

$$K_{ij}^{t+T} = K_{ij}^{0} + \sum\nolimits_{1\cdots T}\left(\left(v_{gen} - v_{con}\right) * \Delta t\right) K_{ij}^{t+T} > 0 \tag{5}$$

- DES:

$$K_{ij}^{t+T} = K_{ij}^{t} - \sum\nolimits_{1\cdots T} v_{con} * \Delta t K_{ij}^{t+T} > 0 \tag{6}$$

- FO:

$$K_{ij}^{t+T} = -\sum\nolimits_{1\cdots T} v_{con} * \Delta t K_{ij}^{t+T} \leq 0 \tag{7}$$

According to the above, K_{ij} in an n-nodes network can be presented as a Secret-key Volume matrix (SV matrix). When a link failure occurs in the network, the secret-key flows of QKPs and the values in SV matrix will be affected. The QKD process on failure-affected link and the secret-key generation process of QKP cannot proceed (i.e., cannot generate secret keys), while the secret keys in failure-affected QKPs are still

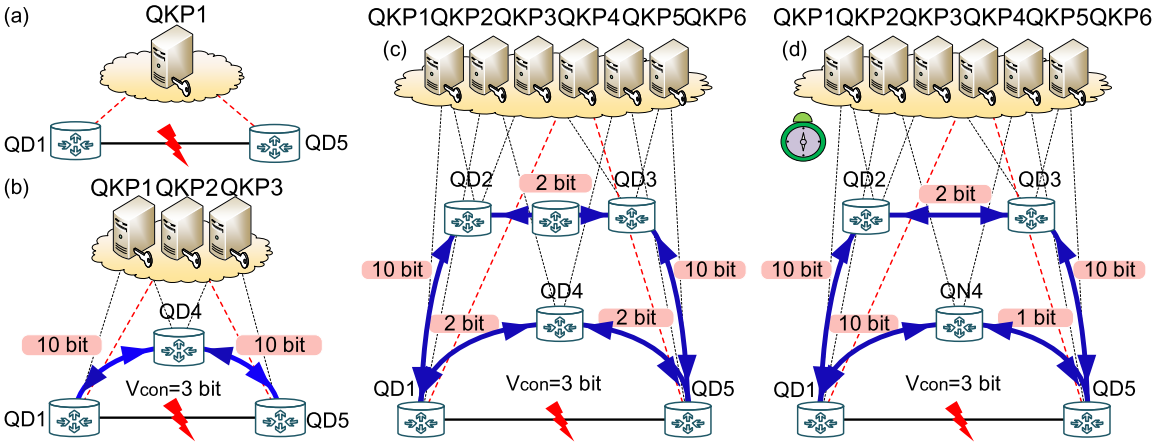

FIGURE 8. Three methods proposed for the recovery of key provisioning services in failure-affected QKPs when a link failure occurred in the network, (a) a link failure occurred, (b) OPRM, (c) MPRM, (d) TWRM.

being consumed. Accordingly, the values of secret-key flows will change with K_{ij} in the formulae in the SV matrix.

$$SV_{Nodes} = \begin{bmatrix} 0 & K_{1,2}^{t+T} & \cdots & K_{1,n}^{t+T} \\ K_{2,1}^{t+T} & 0 & \cdots & K_{2,n}^{t+T} \\ \cdots & \cdots 0 & \cdots & \\ K_{n,1}^{t+T} & \cdots & K_{n,n-1}^{t+T} & 0 \end{bmatrix} \quad (8)$$

IV. SECRET-KEY RECOVERY STRATEGY (SKRS) IN THE NETWORKS

In order to recover failure-affected key provisioning services, a secret-key recovery strategy (SKRS) is designed according to the SKFM. As shown in Fig. 8 (a) – (d), it includes three methods, i.e., one-path recovery method (OPRM), multi-path recovery method (MPRM) and time window-based recovery method (TWRM). The target of these three methods is the re-allocation of secret keys in failure-unaffected QKPs to satisfy the security demands in failure-affected QKPs as much as possible. Specifically, security demand in failure-affected links can be satisfied by the secret keys in one path or several paths. When the secret-key amount in one path cannot fully satisfy the security demands, multiple paths can be used to provide keys at the same time. In addition, since the link fault occurs in the dynamic traffic scene, we designed three algorithms corresponding to the three methods. The specific three methods and the algorithms are described below.

A. ONE-PATH RECOVERY METHOD (OPRM)

The secret-key volume (K_{low}) provided in one path (p) is the secret-key provisioning capability of that path. Taking two failure-affected nodes as the source and destination, multiple paths are calculated as a set P for the recovery. For each p in P, we calculate K_{low}, and check whether path p can satisfy the security demands (K_d). In this process, the paths corresponding to $K_{low} < K_d$ will be removed from P, and the paths corresponding to $K_{low} \geq K_d$ will be sorted in the decreasing order of K_{low}. Then, OPRM tries to find wavelength resources that are capable of the recovery and it stops once the required resources are found. Note that p may have both ESK and PSK, and the paths with ESK are preferred since it can quickly provide keys. For the secret-key provision in

Algorithm 1 OPRM Algorithm

Input: $G(V, L, W, P, P')$, $P_{ij}(v_{gen}, v_{con}, K_{ij})$ $ij \in V$, (aff_s, aff_d), k, A, Δt.
Output: one path recovery and wavelength allocation.

1	*update* v_{gen}, v_{con} *and* K_{ij} *[[space]] of each* P_{ij}
2	*set Paths* ← *K-shortest paths* (aff_{src}, aff_{dest})
3	**for all** *path* ∈ *Paths* **do**
4	*check the* K_{low} *of QKPs in the path*
5	**end for**
6	*order the paths according to* K_{low}
7	**for all** *path* ∈ *Paths* **do**
8	**if** $K_{low} > A$ **then**
9	**if** *available wavelengths in the path* ≠ ∅ **then**
10	*randomly select one of available wavelengths*
11	*break*
12	**else end if else end if**
13	**if** *Paths* = ∅ **then end if**
14	*check* l_i *of the path*
15	*set the links provided* $ESK \longrightarrow L_{ESK}$
16	**for** all $l_i \in L_{ESK}$ **do**
17	**if** *available wavelengths in the path* ≠ ∅ **then**
18	*randomly select one of available wavelengths*
19	**break**
20	**else end if**
21	**for all** $l_i \notin L_{ESK}$
22	**if** *available wavelengths in the path* ≠ ∅ **then**
23	*randomly select one of available wavelengths*
24	*break*
25	**else end if else end if**
26	**end for**

failure-unaffected QKPs, it is necessary to increase the wavelength used for its secret-key generation to replenish the consumed keys. Thus, when it comes to wavelength allocation, two parts of secret keys need to be considered, i.e., the secret keys for the recovery of key provisioning services and the recovery-consumed secret keys. As shown in Fig. 8(b), when the link between QD1 and QD5 with 3-bit security demands fails, path QD1->QD4->QD5 with $K_{low} = 10$ bit can be chosen to provide the secret-key resources and wavelength resources, and the secret-keys between QD1-QD4 and QD4-QD5 will be increased by more wavelength construction for secret-key generation. If no path is found, we switch to MPRM. The specific algorithm 1 is designed for the OPRM.

B. MULTI-PATH RECOVERY METHOD (MPRM)

MPRM use multiple paths as a path group for recovering the failed key distribution services. Different from OPRM, MPRM need to check whether the sum of K_{low} in set P can meet K_d. If so, MPRM takes the paths that can satisfy the K_d as the candidate for the recovery; otherwise, go to TWRM. As with MPRM, more wavelength resources need to be allocated to each link in the selected paths for secret-key generation. As shown in Fig.8 (c), when no single path has more than 3 bit secret keys, two paths (i.e., QD1->QD4->QD5 and QD1->QD2->QD3->QD5) with 4 bit secret keys can jointly provide secret keys. Algorithm 2 is corresponding to the MPRM.

C. TIME WINDOW-BASED RECOVERY METHOD (TWRM)

Since the volume of existing secret keys changes over time, we designed TWRM by updating the secret-key amount to re-calculate one path or several paths through the steps in OPRM or MPRM. The OPRM is performed first to find a path with enough secret keys and available wavelengths, and then MPRM is performed to find several paths to provide secret keys together. These two methods are executed during the time window until they are successful. The calculated paths by them are put into set Pall, and then select the path with biggest K_{low} as the recovery paths. As shown in Fig. 8 (d), the number of secret keys in the QKPs in the network are updated over a time window and the recovery path or paths may be determined by OPRM or MPRM. Algorithm 3 corresponding to the TWRM is shown in the following table.

D. THE COMPLEXITY OF OPRM, MPRM AND TWRM

We evaluate the complexities of the three recovery algorithms as follows. Within one loop, the conditional expression is run at most $|V|$ times. There are two loops in OPRM and MPRM and one loop in TWRM. Thus, the complexity of OPRM algorithm is $O\left(K + V + KV^2\right)$, and the complexity of MPRM algorithm is $O\left(K + V + KV^2\right)$. Since the complexity of TWRM algorithm depends on the times (n) of retrying OPRM and MPRM, so its complexity is $O\left(\left(K + V + KV^2\right)^n\right)$. Although the complexity of OPRM and MPRM are the same,

Algorithm 2 MPRM Algorithm

Input: $G\left(V, L, W, P, P'\right)$, $P_{ij}\left(v_{gen}, v_{con}, K_{ij}\right) ij \in V$, $\left(aff_s, aff_d\right), k, A, \Delta t$.
Output: multi-paths recovery and wavelength allocation.

1	*update* v_{gen}, v_{con} *and* K_{ij} [[*space*]] *of each* P_{ij}
2	*set Paths* ← *K-shortest paths* (aff_{src}, aff_{dest})
3	**for all** *path* ∈ *Paths* **do**
4	*check the* K_{low} *of key pools in the path*
5	**end for**
6	*order the paths according to* K_{low}
7	**if** K_{low} *of the path* $> A$ **then**
8	$V_{accu} += K_{low}$
9	**if** $V_{accu} > A$ **then**
10	**if** *available wavelengths in the path* $\neq \emptyset$ **then**
11	*randomly select one of available wavelengths*
12	**else end if else end if**
13	**if** *Paths* $= \emptyset$ **then**
14	**end if**
15	*check* l_i *of the path*
16	*set the links provided* $\boldsymbol{ESK} \longrightarrow L_{ESK}$
17	**for** all $l_i \in L_{ESK}$ **do**
18	**if** *available wavelengths in the path* $\neq \emptyset$ **then**
19	*randomly select one of available wavelengths*
20	**break**
21	**else end if**
22	**for all** $l_i \notin L_{ESK}$
23	**if** *available wavelengths in the path* $\neq \emptyset$ **then**
24	*randomly select one of available wavelengths*
25	*break*
26	**else end if else end if end for**

OPRM is suitable for general topology and MPRM is preferred to be used in large-scale topology with more nodes and links to be successfully selected. TWRM is preferred to be used in small-scale topology since it is at the cost of time to retry and has little demand for more nodes and links.

V. SIMULATION PERFORMANCES

To evaluate the validity of OPRM, MPRM, and TWRM algorithms in the QKD-integrated optical networks, we set up a simulation in Visual Studio 2015 with C++ language. As shown in Fig. 9, network topologies in the simulation are National Science Foundation network (NSFnet, 14 nodes and 21 links) and United States network (USnet, 24 nodes and 42 links). The numbers of nodes pairs with ESK are set as a parameter and are selected from the nodes in two topologies according to random distribution. The other nodes generate PSK only. The secret-key generation and consumption are coordinated by QKP. For the settings of QKP, without losing generality, two parameters (i.e., v_{gen} and v_{con}) are set to a fixed value and a random value to present the universality of the SKRS, and K_{ij} changes with these two parameters. The specific settings for the simulation are shown in Table 2. According to these, the performances of eight cases (i.e., the

Algorithm 3 TWRM Algorithm

Input: $G = (V, L, W, P, P')$, $P_{ij}(v_{gen}, v_{con}, K_{ij})\ ij \in V$, $(aff_s, aff_d), k, A, \Delta t, n$.
Output: one path or multi-path recovery and wavelength allocation.

```
update v_gen, v_con and K_ij [[space]] of each P_ij
set Paths ← K-shortest paths (aff_src, aff_dest)
for all path ∈ Paths do
    check the K_low of key pools in the path
end for
order the paths according to K_low
counter=0
if counter < Δt then
    update P_ij
    Set P_all initialization
    P_all ← OPRM(); counter++
    P_all ← MPRM(); counter++
        if P_all ≠ ∅ then
            order the Pall according to K_low
            select the first path or paths in P_all
        else failed
    end if
end if
```

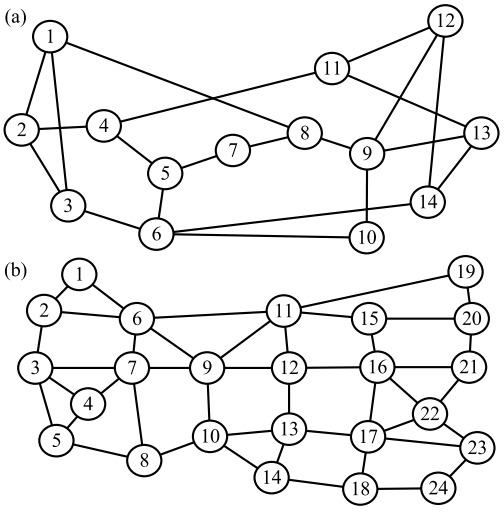

FIGURE 9. Two topologies, (a) NSFnet, (b) USnet.

TABLE 2. Parameters.

Setting	Value
Numbers of paths	3
Numbers of QC	10
Numbers of MC	10
v_{gen} between each pair of links	6 or [5, 7] per time unit
v_{con} between each pair of links	[0, 6], [0, 8], [0, 10] and [0, 12] per time unit
Δt	3 time units

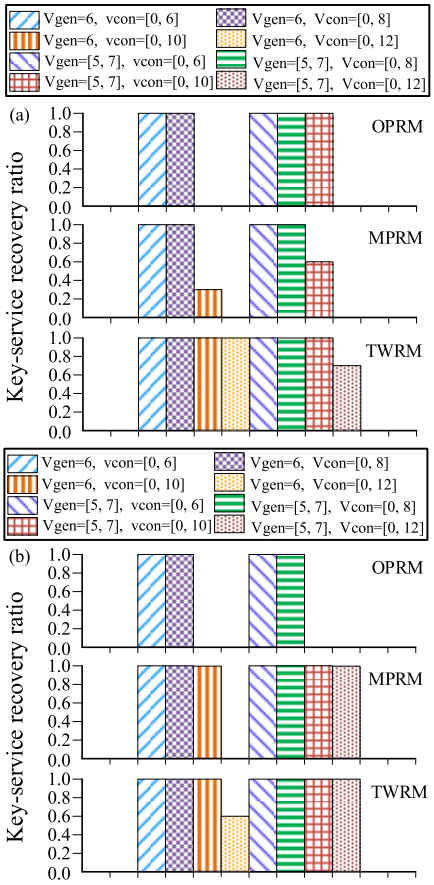

FIGURE 10. The key-service recovery ratio with different v_{gen} and v_{con} in (a) NSFnet and (b) USnet.

arrangement combination of v_{gen} and v_{con}) are simulated and compared in terms of the successful recovery ratio, secret-key recovery degree, wavelength consumption ratio, and secret-key consumption ratio.

A. KEY-SERVICE RECOVERY RATIO

Fig. 10 shows key-service recovery ratio, it is ratio of the numbers of successfully recovered key provisioning services to the total number of failure-affected key provisioning services. For $v_{gen} = 6$, all of three methods can effectively recover the services when v_{con} is in range [0, 6] or [0, 8]. When v_{con} increases to range [0, 10] and [0, 12], only MPRM and TWRM can recover the failure-affected services. Specifically, MPRM can recover parts (30%) of failure-affected key provisioning services which cannot be recovered by OPRM at all (0%), and TWRM can recover all of failure-affected services (100%). This is because MPRM can provide secret keys for failure-affected services as far as possible, and TWRM can provide the probability for the recovery with enough secret keys and available wavelengths through the constant update operation during the time window. Also, for v_{gen} in range [5], [7], the difference with $v_{gen}= 6$ is that TWRM can recover the services when v_{con} is in range [0, 12]. This is because the recovery depends on the secret-key volume

in failure-unaffected QKPs, and secret-key volume fluctuates from time to time. Moreover, the key-service recovery ratios of v_{gen}= [5, 7] and v_{gen}= 6 can verify the recovery effectiveness of the algorithms. It is clear that three proposed methods can recover the services in different cases. The ratios are the same in NSFnet and USnet.

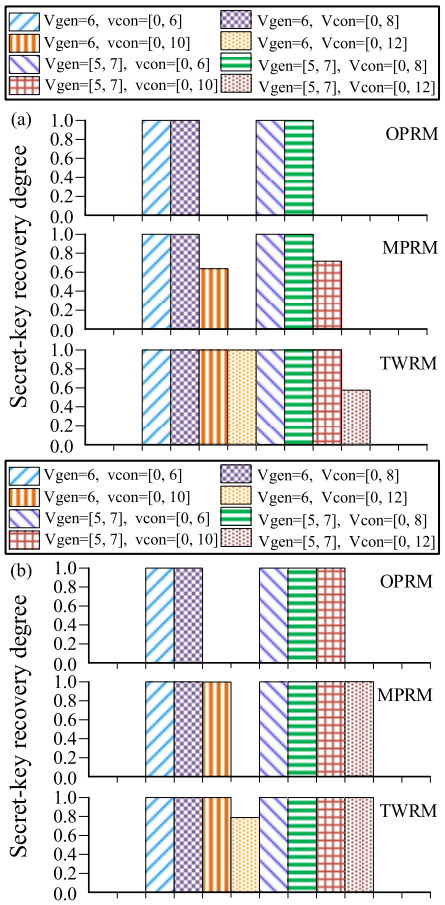

FIGURE 11. The secret-key recovery degree under different v_{gen} and v_{con} in (a) NSFnet and (b) USnet.

B. SECRET-KEY RECOVERY RATIO

Fig. 11 shows secret-key recovery degree in failure-affected QKPs. It is the ratio of successfully recovered amounts of secret keys to the total failure-affected amounts of secret keys. As shown in Fig. 11 (a), it is observed that OPRM can recover the secret keys in failure-affected QKPs completely under the combination of $v_{gen} = 6$ with $v_{con} = [0, 6]$ and [0, 8]. For the combination of $v_{gen} = 6$ with $v_{con} = [0, 10]$, OPRM cannot provide secret keys at all while MPRM should be required for the recovery with 60% secret-key provision. When it comes to v_{gen}= 6 with $v_{con} = [0, 12]$ only, TWRM can recover almost 100% secret keys in failure-affected QKPs. This is because there are keys in QKPs and the secret-key replenishment will be left to find routes easier when the range of v_{con} is bigger than v_{gen}. Similar to the key-service recovery ratio, secret-key recovery ratio of $v_{gen} = 6$ and $v_{gen} = [5, 7]$ have similar trends. In addition, with the increasing v_{con}, the recovery ratio gradually decreases since more QKPs in the network had less K_{ij} to support the secret-key replenishment. From these, it is clear that the recovery degree of TWRM outperforms OPRM and MPRM but at the cost of time units used for the time window. Also, MPRM has a better recovery performance than OPRM since more routes were allocated to complete the recovery of key provisioning services. These performances are the same in the USnet shown in Fig. 11 (b).

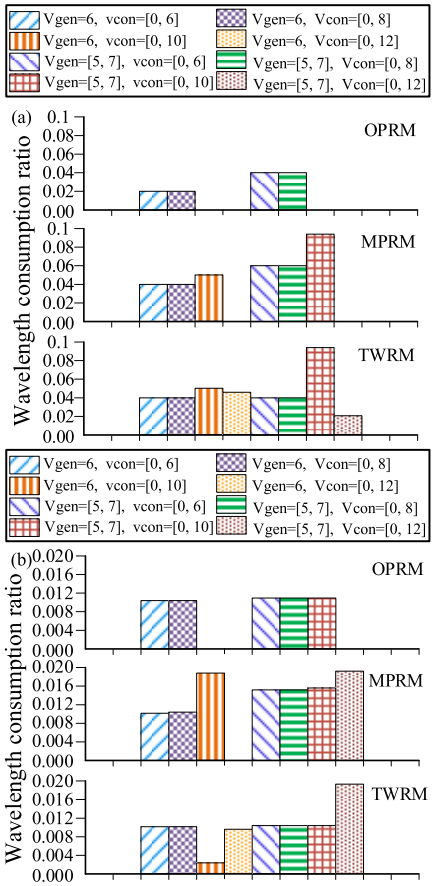

FIGURE 12. The wavelength consumption ratio used for the recovery in (a) NSFnet and (b) USnet.

C. WAVELENGTH CONSUMPTION RATIO

Fig. 12 shows the wavelength consumption ratios used for the recovery with different v_{gen} and v_{con} in the network. Since key-service recovery ratios are existed in several combinations of v_{gen} and v_{con}, partial combinations have wavelength consumption ratio. Furthermore, the trend of wavelength consumption ratio has a similar trend to that of secret-key recovery degree. This is because the range of v_{gen} frees up more selection space for the selection of recovery resources, and bigger v_{gen} means more secret keys with more wavelength consumption. Moreover, compared to OPRM, MPRM generally consumes more wavelength resources since more paths are calculated as the recovery paths, and TWRM has unstable ratios since one of OPRM and MPRM might be used for

the recovery. On the contrary, the wavelength consumption ratios used for the normal generation of PSK and ESK are opposite to that of the recovery. This is because more quantum channels can be used for the generation of PSK and ESK when no failure occurs in the network. Thus, there is a trade-off that exists between the recovery and the delivery of normal QKD on wavelength resources. The performances in USnet are the same with NSFnet.

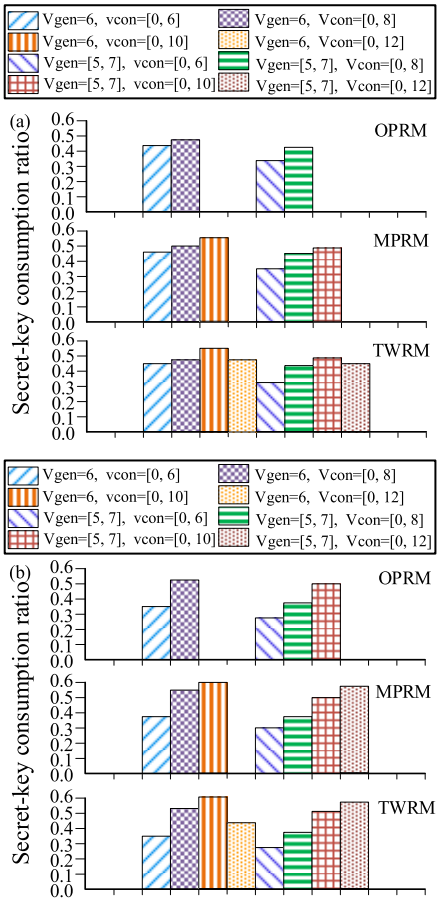

FIGURE 13. The secret-key consumption ratio of recovery-supported QKPs in (a) NSFnet and (b) USnet.

D. SECRET-KEY CONSUMPTINO RATIO

As shown in Fig. 13, it is the ratio of successfully recovered key volume to the total failure-affected secret-key volume with different v_{gen} and v_{con} in two topologies. No matter which method among OPRM, MPRM, and TWRM was performed, the secret-key occupancy at $v_{gen} = 6$ is generally higher than that of $v_{gen} = [5, 7]$. The reason of that is random v_{gen} has a greater probability to generate more K_{ij} in each QKPs. Also, the secret-key consumption ratio of OPRM is less than MPRM, because more QKPs are used for the secret-key replenishment in MPRM which have a similar trend with wavelength consumption ratio. TWRM combines the advantages of OPRM and MPRM at the cost of time. Fig. 14 shows the remaining secret-key ratio of recovery-supported QKPs. The K_{ij} of QKPs are mainly used for their

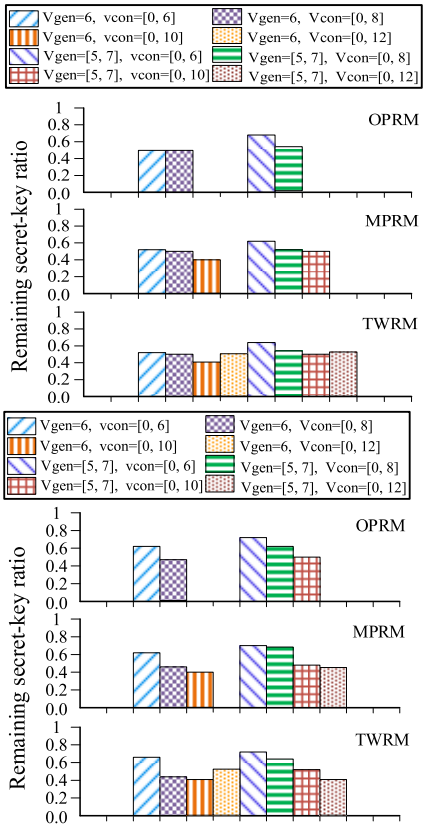

FIGURE 14. The remaining secret-key ratio of recovery-supported QKPs in (a) NSFnet and (b) USnet.

corresponding security demands, when a link failure occurred in the network, each QKP has a probability to be selected as recovery-supported QKP to provide secret keys as much as possible. Then, the remaining secret keys in the recovery-supported QKPs are necessary to be shown. Thus, it is clear that the ratio becomes lower as the range of v_{gen} is bigger. Also, MPRM occupies more secret keys than OPRM due to the reason mentioned in Fig. 13. The performances in Fig. 14 and Fig. 13 are opposite, and it shows that a trade-off exists between the recovery and the generation of secret keys.

VI. CONCLUSION

To strengthen the resiliency of key provisioning services, this paper studied the resilient QKD-integrated optical networks against a single link failure. By analysing and quantifying the key provisioning services, we constructed the network model and secret-key flow model (SKFM). Based on it, a secret-key recovery strategy (SKRS) including three algorithms (i.e., OPRM, MPRM, and TWRM) is designed to strengthen the network. OPRM, MPRM, and TWRM can recover the key provisioning services subject to the availability of wavelength resources and secret-key resources. We also evaluated and verified the performances of the three algorithms in terms of key-service recovery ratio, secret-key recovery degree, wavelength consumption ratio, and secret-key consumption ratio. Simulation results show that three algorithms can recover

key provisioning services in different degrees while requiring more wavelength resources and secret-key resources. Specifically, MPRM outperforms OPRM and TWRM outperforms MPRM, and the occupied wavelength resources and secret-key resources are increased for a better recovery performance. More works related to the resiliency of QKD-integrated optical networks will be further investigated in the future.

REFERENCES

[1] B. Kantarci and H. T. Mouftah, "Bandwidth distribution solutions for performance enhancement in long-reach passive optical networks," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 3, pp. 714–733, 3rd Quart., 2012.

[2] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2016.

[3] M. J. O'Mahony, C. Politi, D. Klonidis, R. Nejabati, and D. Simeonidou, "Future optical networks," *J. Lightw. Technol.*, vol. 24, no. 12, pp. 4684–4696, Dec. 2006.

[4] K. A. G. Fisher *et al.*, "Quantum computing on encrypted data," *Nature Commun.*, vol. 5, Jan. 2014, Art. no. 3074.

[5] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photon.*, vol. 8, no. 8, pp. 595–604, Jul. 2014.

[6] D. Rosenberg *et al.*, "Long-distance decoy-state quantum key distribution in optical fiber," *Phys. Rev. Lett.*, vol. 98, no. 1, Jan. 2007, Art. no. 010503.

[7] P. A. M. Dirac, *The Principles of Quantum Mechanics*, 3rd ed. Oxford, U.K.: Clarendon Press, 1947.

[8] J. Mora *et al.*, "Simultaneous transmission of 20×2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON," *Opt. Express*, vol. 20, pp. 16358–16365, Jul. 2012.

[9] K. Yoshino *et al.*, "High-speed wavelength-division multiplexing quantum key distribution system," *Opt. Lett.*, vol. 37, no. 2, pp. 223–225, Jan. 2012.

[10] I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10Gb/s WDM-PON," *Opt. Express*, vol. 18, no. 9, pp. 9600–9612, Apr. 2010.

[11] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[12] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.*, vol. 84, p. 3762, Apr. 2004.

[13] D. Stucki *et al.*, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New J. Phys.*, vol. 11, no. 2, Mar. 2009, Art. no. 075003.

[14] B. Korzh *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photon.*, vol. 9, no. 3, pp. 163–168, 2014.

[15] H.-L. Yin *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, Nov. 2016, Art. no. 190501.

[16] Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu, and J. Zhang, "Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)," *Opt. Express*, vol. 25, no. 22, pp. 26453–26467, Oct. 2017.

[17] Y. Zhao *et al.*, "Resource allocation in optical networks secured by quantum key distribution," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 130–137, Aug. 2018.

[18] A. Aguado *et al.*, "Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources," *J. Lightw. Technol.*, vol. 35, no. 8, pp. 1357–1362, Apr. 2017.

[19] W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, and A. Tomita, "Technologies for quantum key distribution networks integrated with optical communication networks," *IEEE J. Sel. Topics Quantum Electron.*, vol. 15, no. 6, pp. 1591–1601, Nov./Dec. 2009.

[20] H. Wang *et al.*, "Protection schemes for key service in optical networks secured by quantum key distribution (QKD)," *J. Opt. Commun. Netw.*, vol. 3, no. 11, pp. 67–78, Mar. 2018.

[21] Y. Cao *et al.*, "Time-scheduled quantum key distribution (QKD) over WDM networks," *J. Lightw. Technol.*, vol. 36, no. 16, pp. 3382–3395, Aug. 2018.

[22] H. Wang, Y. Zhao, X. Yu, B. Chen, and J. Zhang, "Resilient fiber-based quantum key distribution (QKD) networks with secret-key reallocation strategy," in *Proc. OFC*, San Diego, CA, USA, 2019, pp. 1–3, Paper W2A.25.

[23] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: Challenges and solutions [Invited]," *Opt. Express*, vol. 26, no. 18, pp. 24260–24273, Sep. 2018.

[24] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, Jul. 2009, Art. no. 075001.

[25] M. Dianati and R. Alleaume, "Transport layer protocols for the Secoqc quantum key distribution (QKD) network," in *Proc. LCN*, Dublin, Ireland, Oct. 2007, pp. 1025–1034.

[26] O. Maurhart, "QKD networks based on Q3P," *Applied Quantum Cryptography* (Lecture Notes in Physics). Berlin, Germany: Springer, 2010, p. 797.

[27] M. Dianati and R. Alleaume, "Architecture of the Secoqc quantum key distribution network,"in *Proc. ICQNM*, Guadeloupe City, Guadeloupe, 2007, p. 13.

[28] M. Dianati, R. Alléaume, M. Gagnaire, and X. Shen, "Architecture and protocols of the future European Quantum key distribution network," *Secur. Commun. Netw.*, vol. 1, no. 1, pp. 57–74, Jan. 2008.

[29] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, "Quantum repeaters and quantum key distribution: Analysis of secret-key rates," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 5, May 2013, Art. no. 052315.

[30] C. Varnava *et al.*, "An entangled-LED-driven quantum relay over 1 km," *NPJ Quantum Inf.*, vol. 2, Mar. 2016, Art. no. 16006.

[31] W. Stacey, R. Annabestani, X. Ma, and N. Lütkenhaus, "Security of quantum key distribution using a simplified trusted relay," *Phys. Rev. A, Gen. Phys.*, vol. 91, Jan. 2015, Art. no. 012338.

[32] S. Wehner, D. Elkouss, and R. Hanson, "Quantum Internet: A vision for the road ahead" *Science*, vol. 362, p. eaam9288, Oct. 2018.

[33] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014.

[34] A. N. Pinto, N. A. Silva, A. J. Almeida, and N. J. Muga, "Using quantum technologies to improve fiber optic communication systems," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 42–48, Aug. 2013.

[35] D. Elkouss, J. Martinez-Mateo, A. Ciurana, and V. Martin, "Secure optical networks based on quantum key distribution and weakly trusted repeaters," *J. Opt. Commun. Netw.*, vol. 5, no. 4, pp. 316–328, Apr. 2013.

[36] R. V. Meter and J. Touch, "Designing quantum repeater networks," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 64–71, Aug. 2013.

HUA WANG received the B.S. degree from Xiangtan University (XTU), in 2016. She is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications (BUPT). Her research interests include elastic optical networks, quantum key distribution (QKD), and the survivability of optical networks integrated with QKD.

YONGLI ZHAO received the B.S. degree in communication engineering and the Ph.D. degree in electromagnetic field and microwave technology from the Beijing University of Posts and Telecommunications (BUPT) in 2005 and 2010, respectively, where he is currently a Professor with the Institute of Information Photonics and Optical Communications. He has published over 150 journal and conference articles. His research interests include software-defined optical networks, flexi-grid optical networks, and network virtualization.

XIAOSONG YU received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), China, in 2015, where he is currently an Assistant Professor with the Institute of Information Photonics and Optical Communications (IPOC). His research interests include spatial division multiplexing-enabled elastic optical networks (SDM-EONs), software-defined optical networking (SDON), data center networking, and optical network security.

AVISHEK NAG is currently an Assistant Professor with the School of Electrical and Electronic Engineering, University College Dublin, Ireland. His research interests include cross-layer optimization in wired and wireless networks, network reliability, the mathematics of networks, network virtualization, software-defined networks, machine learning, data analytics, and the Internet-of-Things.

ZHANGCHAO MA received the B.S. and Ph.D. degrees from the Beijing University of Posts and Telecommunications (BUPT), in 2006 and 2011, respectively. He currently serves as the standard Director of Chinese Academy of Sciences Quantum Network Co., Ltd., and the Vice Chair of the CCSA ST7 Quantum Information Processing Sub-Group, committed to promoting the standardization of quantum secure communication and the construction of QKD networks.

JIANQUAN WANG is currently a Professor and a Ph.D. Supervisor with the Beijing University of Posts and Telecomm. He is also currently with CAS Quantum Network Co., Ltd. He is a member of the National Broadband Wireless Access Network Engineering Technology Research Center, Engineering and Technology Committee, the China Institute of Communications, the Optical Communication Committee, and the Wireless and Mobile Communication Committee.

LONGCHUAN YAN was born in 1978. He is currently pursuing the Ph.D. degree with the Institute of Information Engineering, Chinese Academy of Sciences. His main research interests include cloud computing, energy-efficiency, machine learning, and distributed computing.

JIE ZHANG received the bachelor's degree in communication engineering and the Ph.D. degree in electromagnetic field and microwave technology from BUPT. He is currently a Professor and the Vice Dean of Information Photonics and Optical Communications Institute, Beijing University of Posts and Telecommunications (BUPT), China. He has published over 300 technical papers. He has authored eight books, submitted 17 ITU-T recommendation contributions, and six IETF drafts. He holds 17 patents. He has served as a TPC member of a number of conferences such as ACP, OECC, PS, ONDM, COIN, and ChinaCom. His research interests include architecture, protocols, and standards of optical transport networks.