Secret-Key Reservation Strategy for Security Resilience in Passive Optical Networks

Hua Wang
State Key Laboratory of IPOC, Beijing University of Posts and Telecommunications
Beijing, 100876, China
Huawang@bupt.edu.cn

Yongli Zhao
State Key Laboratory of IPOC, Beijing University of Posts and Telecommunications
Beijing, 100876, China
Yonglizhao@bupt.edu.cn

Xiaosong Yu
State Key Laboratory of IPOC, Beijing University of Posts and Telecommunications
Beijing, 100876, China
xiaosongyu@bupt.edu.cn

Mengxi Zhang
State grid economic and technological research insititute co.LTD.
Beijing, 100876, China
zhang_mxi@163.com

Jiangsheng Li
State grid economic and technological research insititute co.LTD.
Beijing, 100876, China
lijiangsheng@chinasperi.sgcc.com.cn

Guangxiang Jin
State grid economic and technological research insititute co.LTD.
Beijing, 100876, China
jinguangxiang@chinasperi.sgcc.com.cn

***Abstract*—Regarding the security of PONs, a secret-key reservation strategy is proposed to supply keys in failure duration for users to achieve security resilience. Simulation results show its effectiveness with various performances compared to the benchmark.**

Keywords—PONs, quantum key distribution, resilience, time-slot allocation.

I. INTRODUCTION

Nowadays, emerging requirements put forward by 5G and F5G techniques, more and more end users will be gradually allowed with their devices to access networks. It makes access networks become important, and fiber always plays the role of a major transmission carrier in part of it. Traditional optical access networks are classified into active optical networks and Passive Optical Networks (PONs) according to the used devices [1]. Among these, PON was a popular one and raised researchers' attention due to its benefits of low cost and better universality in practical applications and thus. Lots of techniques are explored to guarantee end users' requests. Among these, security becomes one of the important items that should be considered in this case, especially when it accesses devices from various sources.

In previous decades, there are many studies working on PONs. Most of them focus on the fairly responding mechanisms for multi-users in PONs, and thus designed lots of bandwidth allocation protocols, one of which is known as the IPACT [2]. While as more and more applications are developed, it will easily occur a lot of online services sending from multiple sources to transmit in PONs. Most of them are tending to be sensitive and have a strong relationship with their personal property, government, or military services. In this case, it is necessary to guarantee the security of service delivery in PONs. Given the open environments of PONs, service transmission faces a serious challenge of security to against illegal attacks like eavesdropping [3]. In response to it, services are always having encryptions with secret keys generated by the AES algorithms in computers against eavesdropping. While it will be easily threatened by some newly emerging techniques which are explored with advanced computation ability nowadays. For example, quantum supremacy [4] was proposed by Google in 2019, which is a super-computation technique that challenged traditional encryption ways. This is because traditional encryption ways rely on mathematical complexity which can be easily conquered by strong computation ability. Therefore, it is necessary to enhance the security of service delivery in PONs.

As a promising option, Quantum Key Distribution (QKD) can generate more securer keys than traditional ones. Its security is guaranteed by the physical mechanisms of quantum bits, i.e., the no-cloning theorem, the uncertainty principle, and so on [5]. Generally, QKD can be performed in two different ways, i.e., discrete-variable QKD and continuous-variable QKD. Among these, the former can perform a longer distance than the latter, but with a relative-low key rate. Given the technical maturity, we formally consider the former way as the secret-key generation to secure PONs [6, 7] in this paper. At the same time, there are various QKD protocols like BB84 which are also helpful to improve QKD performances like distribution distance and key rate. Attacked by the above benefits, QKD is seen as one potential way to generate secret keys to guarantee the security of PONs. Moreover, the scale of a general PON is less than 50 km which also makes PON become a suitable application scenario for QKD. Based on it, there are lots of existing studies on the exploitation of QKD in PONs and various experiments of QKD deployments in the physical layer. Although these studies illustrated the feasibility of QKD in PONs, it will still come out a serious problem how to allocate fixed numbers of resources to generate secret keys to satisfy the key-volume requirements in practical. Aimed at it, the author studied and proposed QKD secret-key allocation strategies for multi-users in PONs in 2020 [8]. In this paper, we try to further learn more about secret-key allocation in PON, especially in its failure case to enhance the resilience of secret-key provision. This is an important topic since every network will inevitably suffer failures either caused by accidental fiber cutting or natural disasters. It should consider how to continue providing the key without losing its meaning in a failure scenario. Therefore, the problem of how to guarantee sufficient secret-key provision for PONs in a failure scenario should be studied. The failure scenario in this paper was considered with single fiber cutting which is worthy of study and can be illustrated as an example.

In this paper, we focus on the Secret-key Reservation (SR) strategy to supply keys during failure duration for security resilience in PONs. Simulation results show its effectiveness with result performances in terms of Secret-Key Provision (SKP) failed ratio, backup key volume, and successful SKP ratio. The rest of the paper is organized as follows. Section II overviewed the background of QKD in PONs and the failure

scenario. In Sec. III, we designed SR strategy with dynamic time-slot allocation. In Sec. IV we discussed numerical simulation results. In Sec. V, we draw the paper's conclusion.

II. QKD-SECURED PON

A. Background of QKD

QKD can be directly performed from point to point which can be seen as two adjacent users sharing secret keys. For instance, there are two points, i.e., named Alice and Bob. They are arranged with pairs of QKD Transmitter (QT) and QKD Receiver (QR) and connected through fibers with each other. The fibers include multiple wavelengths which are specified for QKD by using wavelength-division multiplexing. When it comes to DV-QKD, the implementation of it formally requires two types of wavelengths including quantum channel (i.e., placed at approximately 1510 nm for qubits) and optical channel (i.e., placed at approximately 1530 nm for optical bits). Considering the experimental data under such settings, a quantum encryption system can achieve about Mb/s key rates in 200 Gb/s bandwidth over 100-km fiber. This experiment also imposes a condition that the quantum channel needs to be separated from the other channels at least 100 GHz. Based on the above conditions, there are some studies further learning about optical time-division multiplexing [9, 10], multi-mode and multi-core multiplexing over wavelengths in fiber for QKD. Also, since nowadays QKD technique is hard to match the practical application requirements limited by the distance and key rate, there are some other ideas like the constructions of quantum key pools (QKPs) to cache keys and take keys out for users as one kind of soft buffer. In this paper, in order to alleviate the burstiness of services in PONs and their consequent security requirements, it is better to consider QKP for key storage in our basic model.

B. Architecture of QKD-secured PONs

Typically, the consistency of PONs has several basic items. The first one is the optical line terminal (OLT) in the local center for centralized control and management. The second is the Optical network unit (ONU) on the user side. The third one is the passive optical splitter (POS) and combiner to combine or split the optical signals from several branches on the user side into one branch to the OLT. These three items are connected through different fibers, which also consist of multiple wavelengths. Similarly, these wavelengths can be further divided into serial time slots in avoidance of the conflict of resource allocation of multiple users. This conflict is always caused by the unsuitable cycle period of the allocation of fixed resources to different users in turn. In order to perform QKD in PONs, it is first to deploy it with its implementation devices. Considering the original architecture of PONs, there are three potential QKD deployments in PONs. As shown in Fig. 1 (a), the first one is to put QR in the OLT and QT in the ONU. It can use specified wavelengths in the fiber between OLT and ONU. The implementation of it is similar to the manner of one OLT with multiple ONUs. Multiple QTs will be allowed to connect QR in turn achieved by optical time-slot division. During the specified time slots, one QT can implement QKD with the QR to generate secret keys. Correspondingly, the QR will be configured with multiple QKPs to store the secret keys generated between different QTs. Similarly, the time-slot allocation of them is also important which will allow the on-demand secret-key provision for users. It is obvious to see this kind of deployment is cost-efficient to share QR which is expensive among multiple users. The second deployment is to put QT in the local center and QR in the ONU, which will use multiple QRs. The third deployment is to put QT and QR both in the OLT and ONUs. It can provide relative-quick secret-key generation since the key rate has positive correlation to the numbers of QT and QR pairs. In this paper, we consider the first one, and the secret-key generation here is unidirectional between OLT and ONUs.

C. Security resilience of QKD-secured PONs

In the architecture of QKD in PONs, it will enviably occur kinds of failures like fiber cutting. Among these, single cutting is one representative and a relative-simple case. Under this situation, there are two possible links that occurred with single

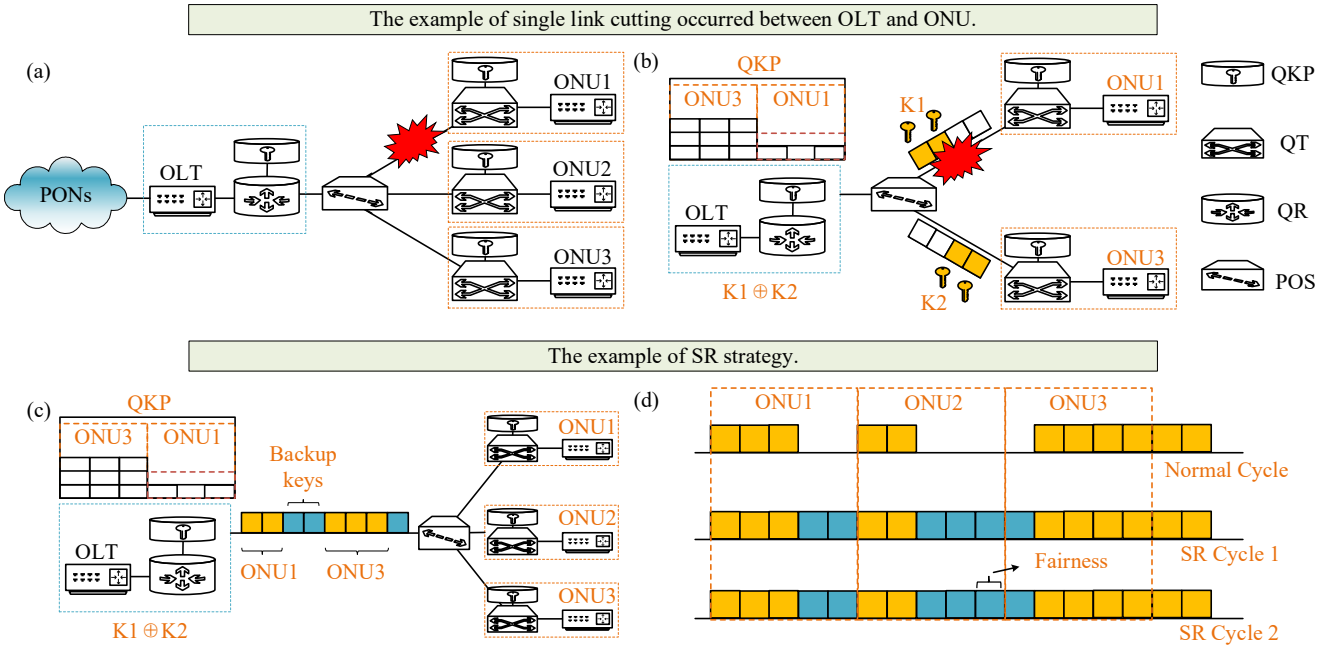

Fig. 1. The examples of (a) single link cutting occurred between the Optical Line Terminal (OLT) and Optical Network Unit (ONU), (b) interruption of Quantum Key Distribution (QKD) between Passive Optical Splitter (POS) and Transmitter (QT), (c) Secret-key Reservation (SR) strategy.

fiber cutting, i.e., respectively in the links between ONU-POS and POS-OLT links. These two kinds of link failures will result in different consequences on the secret-key prevision, which is an interesting topic and worthy of study. Judging by the results, the former will only disrupt secret-key generation between one user and OLT. While the latter will apparently disrupt all of the secret-key generations for the whole users. Both of these two will interrupt secret-key generation, putting the user's secret-key provision at risk, further weakening the security guarantee of QKD in PONs. Given by the former is the basis and decomposition of the latter, we focus on the former in this paper. More specifically, once the single fiber cutting occurs, OLT and the influenced user cannot generate secret keys as normal. Especially during time periods of the repairment, the user can only use the previous secret keys stored in their QKP which is a certain surplus. In this case, we need to consider the resilience of the security guarantee (namely security resilience) coming from QKD in failure scenarios when applying it in PONs. Based on the above statement, the following will give the problem statement.

D. Problem statement

Single link failure would obviously interrupt the secret-key generation. It would likely occur following three kinds of cases. As for the first one, if the surplus of secret keys is few and the user security requirements are high, it should design a strategy to maintain the ability of secret-key provision. As for the second case, if the surplus of secret keys is still many and the requirements are also high, the normal secret-key provision may be possibly maintained to satisfy the requirement. Also, it will come to a similar result in the third case, if the surplus of secret keys is low and the requirements also are few, the normal secret-key provision may be maintained. In this view, it is efficient to set the dedicated storage of secret keys in QKPs in advance to avoid the incompetent provision of user requirements.

III. SECRET-KEY RESERVATION ALGORITHM

Regarding the interruption problem of one user's secret-key generation caused by the single link cutting, we designed SR algorithm in this section. As shown in Fig. 1 (b), it shows the SR strategy to generate and prepare extra secret keys for the backup. First, we set the failure duration T_{fail} of single link cutting in PONs to a variable which can be obtained from empirical data and achieved by the prediction of machine learning in some existing studies. Then, there is an calculation of the total backup key volume V_{backup} during T_{fail}. It is counted in general and average amount of it is based on the previous data. Also, this volume can be seen equal to every users. Next, we can have the V_{backup} and the total numbers of time slots also can be calculated with the ratio of V_{backup} with the key rate per time slot k_{rate}. Next, it need a time-slot allocation to generate these keys. The network topology was supposed to $G\left(U, QKP\left(k_{rate}, v_{u\{i,\cdots U\}\_c}\right)\right)$, where U refers to users and two parameters respectively for key rate and key volume. In order to achieve the generation, a certain numbers of time slots will be allocated for QKD which can be randomly insert in the cycle of the normal generation for multiple users. In order to form backup key requests $r_{s\_i}(u_i)$ for U users, and put $r_{s\_i}(u_i)$ into the backup key request set S1. The server collects, respectively calculates the number of time slots that need to be occupied and forms $r_{s\_j}(u_j, v_j, t_s, t_e)$ format, sort these requests into the set S1 to form normal cycle. The secret-key requests will be collected in set S1, and then with random insertion of the time slots for backup keys by judging the occupancy of current network resources. The backup key time slot is inserted without affecting the user's key replenishment. We supposed that the network resource status is idle, and the secret-key requests in set S1 can be traversed for key generation for multiple users. It can be exploited with the time slot reset polling cycle algorithm for backup key supply. In this way, the network time slot resources are occupied by multiple users in SR cycle 1.

Then, the server collects and calculates the amount of backup keys of one user through a given failure duration. It can obtain the number of time slots of backup keys for one user. The server forms the user's backup key request with the number of time slots required for each user's backup key and

TABLE I. SR ALGORITHM.

Input: $G\left(U, QKP\left(k_{rate}, v_{u\{i,\cdots U\}\_c}\right)\right)$, T_{fail}, V_{backup}, k_{rate}, $r_{s\_i}(u_i)$, $r_{s\_j}(u_j, v_j, t_s, t_e)$.

Output: time-slot arrangement for secret-key reservation.

1	Int $T_{fail} = 0$	17	$r_{s\_j} \rightarrow$ S2;
2	**For** (i=1; i<U; i++)	18	Sort the order of S2;
3	$T_{fail} = v_j + +$;	19	**End if end for**
4	$n_{b\_i}=V_{backup}/k_{rate}$	20	**For** (i=1; i<m; i++)
5	Form $r_{b\_i}(u_i, n_{1\_i})$	21	**For** (j=1; j<n; j++)
6	$r_{b\_i} \rightarrow$ S1	22	$Index_{i\_j}=QKP(v_{uj\_c})-(n_{s_j}+n_{b_i})*k_{rate}$
7	**End for**	23	$Index_{i_j} \rightarrow$S3
8	Collect $r_{s\_j}(u_j, v_j, t_s, t_e)$	24	**End for end for**
9	Mark QKP $\left(v_{u\{i,\cdots U\}\_c}\right)$ for u_i	25	**For** (i=1; i<m; i++)
10	**For** （j=1; j<n; j++）	26	**For** (j=1; j<n; j++)
11	$n_{s\_j}=V_j/k_{rate}$	27	**If** ($Index_{i\_j}<Index_{i_{j+1}}$)
12	$r_{s\_j}(u_j, v_j, t_s, t_e, n_{2\_j})$;	28	Counter=j;
13	$r_{s\_j} \rightarrow$ S2	29	**End if End for**
14	**End for**	30	$r_{b_i} \rightarrow$S1;
15	**For** (j=1; j<n; j++)	31	Sort the order of S2;
16	**If** ($QKP(v_{uj\_c}) < QKP(v_{uj+1\_c})$)	32	**End for**

puts it into the set S3 to form SR cycle 2. The server looks at the key supply request set S1 and the backup key request set S2, and calculates the evaluation index $Index_{i\_j}$ of the the location of the time slot occupied by the backup key on the key supply of other users, so as to find a suitable location for backup key generation. The backup key request $r_{s\_i}(u_i)$ puts the impact factor in front of the corresponding request in set S1, and updates set S1 to form a new round-robin cycle including backup key supply.

IV. Simulation Results and Discussion

A. Simulation settings

In this section, simulation verification and result analysis are carried out for the proposed algorithm. Moreover, the two cases i.e., the SR1 with random time-slot insertion and the SR2 for fairness were compared without SR as the benchmark. The simulation is compiled in C++ language in Virtual Studio software. The network topology consisted of 32 users. Each user is equipped with QKP to store keys. QKP indicates that the initial state of the network is full capacity, and the key rate is supposed to be 500 bits per time slot. The arrival of secret-key requests obeys the Poisson distribution, and their key demand is randomly selected in the range [0,500]. When the number of keys in QKP is near the threshold. The simulation set the failure duration to 50 time slots. The simulation evaluates the performance before and after the link failure respectively with different indexes. The Secret-Key Provision (SKP) failed ratio, backup key volume, and successful SKP ratio are used to illustrate the effectiveness of the solution.

B. Simulation results

Fig. 2 (a) shows the SKP failed ratio, which is used to reflect the impact of backup keys on normal key generation. It is caused by the time slot occupation of the backup key, which causes the normal key not to be replenished on time, and the key pool is empty and cannot meet the user's request. It is the ratio of the number of key replenishment failures to the total number of key replenishment times. It can be seen from the figure that as the key request arrival rate increases, the failure rate also increases exponentially. However, the rate of SR strategy 1 is significantly higher than that of SR strategy 2, this is because that SR strategy 1 considers the influence of local key supply on time slot occupation, thus affecting the time slot occupation of subsequent key supply. SR strategy 2 considers the allocation of backup key time slots from a global perspective, which obviously occupied more time slot resources than the performances without SR.

Fig. 2 (b) shows the backup key volume, counted by the average number of time slots from the beginning to the end of the backup key generation. It can be seen from the figure that as traffic load increases, the volumes had fluctuations. The highest volume changing with traffic load was around 160. This is because as the arrival density of secret-key requests increases, the consumption of keys in QKP became faster, and the number of secret-key requests increases. However, the time slot number of network resources is limited. As a result, the efficiency of backup becomes lower. However, when the density of keys reaches a certain level, the volume of network key supply will increase, and network resources will be idle, thereby reducing the efficiency of key backup. The efficiency of SR strategy 2 for backup key supply is better than that of SR strategy 1 because the supply of SR strategy 2 occupies a small number of network redundant time slots and the allocation of time slots is relatively concentrated, so the backup key supply time is short.

Fig. 2 (c) is the successful SKP ratio during the failure duration, which is the ratio of the times of successful SKP for the user during the fault period to the total number of user key requests during the failure duration and is mainly used to display the backup key pair during the failure duration. It can reflect the degree of satisfaction of users with the SKP, which also means the resilience of key supply capabilities in PONs. At the same time, this indicator also reflects the accuracy of the estimated key volume. The indicators are compared in the case of no backup key, the random insertion algorithm of the backup key supply time slot with the backup key, and the reset polling cycle algorithm of the time slot required for the backup key supply. It can be seen from the figure that there is no backup key. During the failure duration, the users' QKP can still provide keys for requests until the consumption is empty and no longer has the ability to supply. This is the security capability of PON described above. It can be seen from the figure that establishing a backup key can effectively extend the ability to supply keys to user requests during failures, thereby improving the resilience of the networks. Compared with SR strategy 1, the successful SKP rate of SR strategy 2 is higher because more time slots were occupied continuously and the backup volume also is high, so that it can quickly and effectively provide keys for user requests.

V. Conclusion

A secret-key reservation strategy is proposed to supply keys in failure duration for users to achieve security resilience in PONs. Simulation results show that the proposed algorithm can effectively provide secret keys via various performances compared to the benchmark.

Acknowledgment

Fig. 2. Simulation results, (a) the failed ratio of secret-key provision in failure duration, (b) the backup key volume, (c) the successful ratio of secret-key provision.

This work has been supported in part by China State Grid Corp Science and Technology Project (5108-202218280A-2-416-XG).

REFERENCES

[1] C. F. La m, Passive optical networks: principles and practice. Elsevier, Ed., 2011.

[2] A. Buttaboni, M. De Andrade, M. Tornatore, A. Pattavina, "Dynamic bandwidth and wavelength allocation with coexisting transceiver technology in WDM/TDM PONs," Optical Switching and Networking, 2016, vol. 21, pp.31-42.

[3] H. Wang, Y. Zhao, X. Yu, Z. Ma, J. Wang, L. Yi, and J. Zhang, "Protection Schemes for Key Services in Optical Networks Secured by Quantum Key Distribution (QKD)," Journal of Optical Communications and Networking, 2018, vol. 11, pp. 67-78.

[4] A. Frank, et al. "Quantum supremacy using a programmable superconducting processor," Nature, 2019, vol. 574.7779, pp. 505-510.

[5] R. Renato, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," Physical Review A, 2005, vol. 72, pp.012332.

[6] H. Wang, Y. Zhao, A. Nag, X. Yu, X. He, and J. Zhang, "End-to-end quantum key distribution (QKD) from metro to access networks," 2020 16th International Conference on the Design of Reliable Communication Networks 2020. IEEE, 2020.

[7] H. Wang, Y. Zhao, and A. Nag, "Resilient Quantum Key Distribution (QKD)-Integrated Optical Networks with Secret-Key Recovery Strategy," IEEE Access, vol.7, pp.60079-60090, 2019.

[8] H. Wang, Y. Zhao, and A. Nag, "Dynamic secret-key provisioning in quantum-secured passive optical networks (PONs)," Optics Express, 2019, vol.9, pp. 2081.

[9] X. Yu, Y. Liu, X. Zou, Y. Cao, Y. Zhao, A. Nag, and J. Zhang, "Secret-Key Provisioning with Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks," Journal of Lightwave Technology, 2022, vol. 44, pp.3530-3545.

[10] X. Yu, X. Liu, Y. Liu, A. Nag, X. Zou, Y. Zhao, and J. Zhang, "Multi-path-based quasi-real-time key provisioning in quantum-key-distribution enabled optical networks (QKD-ON)," Optics Express, 2021, vol. 29, pp. 21225-21239.