Degradation-aware Resilience Strategy for Quantum Key Distribution Co-existence With Classical Communication in Optical Networks

Yuhang Liu
State Key Lab of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
yuhangliu@bupt.edu.cn

Xiaosong Yu
State Key Lab of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
xiaosongyu@bupt.edu.cn

Yongli Zhao
State Key Lab of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
yonglizhao@bupt.edu.cn

Jie Zhang
State Key Lab of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
lgr24@bupt.edu.cn

***Abstract*—In this paper, we study a degradation-aware network resilience strategy for quantum key distribution (QKD) co-existence with classical communications. The secret key rate (SKR) can be improved by *96.4%* on average with the proposed *DS-QKD* strategy in a wavelength division multiplexing (WDM) optical network with 40 wavelength channels.**

Keywords—Quantum key distribution (QKD), degradation-aware, network resilience, co-existence, classical communications

I. Introduction

The accelerated expansion of communication demand is inducing a new technological revolution in data communication area [1]. As one of the world's most important information infrastructures, optical network undertakes most of the user communication services, and the capacity is upgrading from Gb/s to Tb/s [2]. However, with substantial breakthroughs in the field of quantum computing, data communication security based on classical computational complexity is facing severe challenges. In order to ensure high reliability of user communication, various security methods have been proposed.

Based on the uncertainty theorem, QKD can provide theoretically unconditional secured keys to ensure the security of data communication [3]. Since the decoy-state BB84-QKD protocol was proposed, QKD has been deployed and applied in optical networks based on dark fibers. The key technologies of large-scale QKD networking including trusted relay, key management, etc. have been demonstrated in Tokyo QKD network, and China Satellite-to-ground QKD network experiments [4-5]. Generally, the QKD network was initially deployed as a key delivery infrastructure, and dark fibers were mostly used to implement the classical measurement and quantum state transmission for QKD [6]. However, when the application scenarios of QKD are expanded, more point-to-point QKD systems need to be deployed to meet the secret-key demand of data communication, which will bring more investments. Thus, the industry expects to utilize WDM technology to enable QKD and classical communications to share commercial optical fibers, which can complete data communication and key negotiation simultaneously. From the devices' perspective, lightweight chip based QKD transceivers are developed, which are capable of being integrated into existing optical networks. Experiments have shown the prospect of QKD with silicon photonics integrated transmitters and receivers, which greatly reduces the cost for building trusted QKD nodes [7]. For the co-existence of classical communications and QKD communications during transmission, certain scale of experiments have proved the feasibility of the co-propagation with considerable QKD performance [8].

However, to make the prospect come true, optical loss is still an important limitation for co-existence of classical and QKD communications. Basically, we hope that QKD and classical communication can achieve a similar performance (i.e., equivalent communication rate and key generation rate), at least increase the key generation rate as much as possible. Under certain frequency conditions of QKD devices, the existence of interference noise fundamentally limits the photonic efficiency of QKD to produce the final keys, and the high dynamics of classical communication also makes it more serious. The importance is that the compromised photon efficiency will always limit the performance of QKD itself, and until now there is no countermeasures to completely solve this problem, which would become a fundamental factor restricting the network integration.

In recent years, a series of transmission theory studies have proved that the actual SKR will be suppressed by classical signals. It is mainly reflected in the photon crosstalk introduced by the non-ideal characteristics of the devices and the nonlinear interaction between optical signals, mainly including amplified spontaneous emission (ASE) noise, channel crosstalk, Raman scattering, and four-wave mixing (FWM). Based on improvement on transmission systems, the ASE background noise can be easily eliminated by cascading multiplexers and deep notch filters, and crosstalk between channels can be avoided by setting reasonable guard-band (e.g., 200 GHz) between quantum and classical signals [9]. The effect of FWM can be suppressed effectively under a metropolitan distance (e.g., in the unit of more than 10 km). Most experiments prove that Raman scattering becomes an

This work is supported by NSFC project (61971068, 62150032, U22B2026), National Key Research and Development Program of China (2020YFE0200600), Fund of State Key Laboratory of Information Photonics and Optical Communications, BUPT (IPOC2020ZT04).

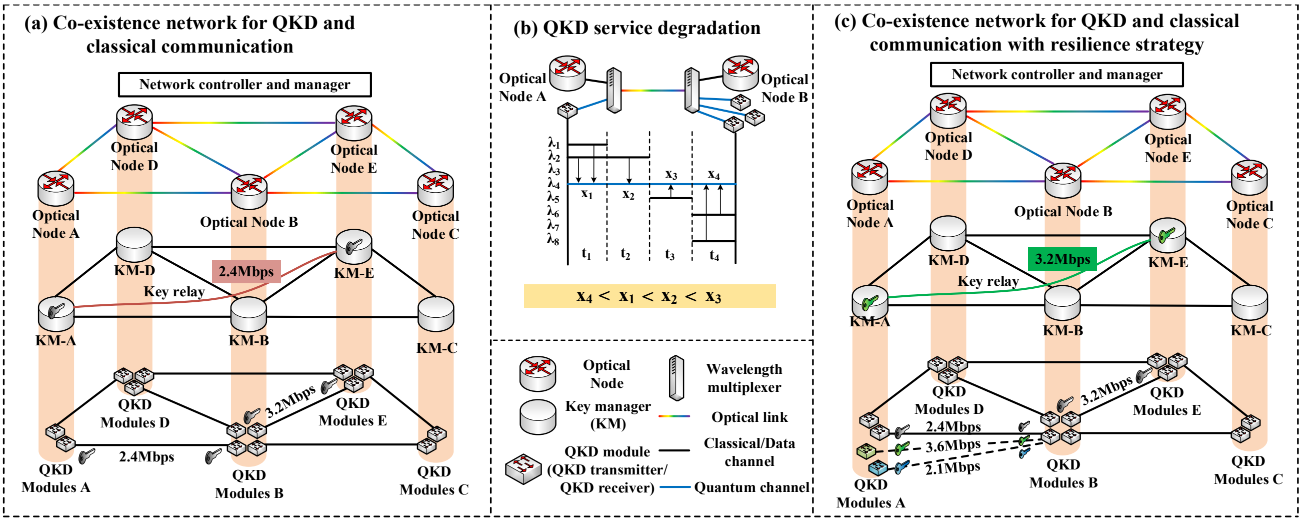

Fig. 1. (a) Optical network for co-existence of QKD and classical data communications; (b) QKD service degradation; (c) optical network for co-existence of QKD and classical data communications with resilience strategy

inevitable main noise source during co-propagation, and its nonlinear spectrum can cover the entire communication wavelength channels with an evenly distributed optical power.

Thus, under most cases of co-existence of QKD and classical communications, the scarce key resource is unable to meet the one-time-pad (OTP) encryption requirement. At the same time, key generation rates would be subject to unavoidable noise and performance fluctuations with the dynamics of classical data communication services. To satisfy the user's key demand, it is difficult to achieve a stable SKR to support the well-organized key life cycles. When SKR is decreases with heavier noise effect, which is referred to the QKD service degradation, corresponding resilience strategies should be supported to recover the network performance with a stable level of SKR as much as possible. It may require the capability of adaptive routing control of classical and quantum communications to dynamically adjust the SKR for stable key provisioning. Considering that QKD is usually a continuous procedure, that is, the classical and quantum channels should be always at a working state. The resilience strategies may need additional QKD modules for pre-configuration of QKD links.

In this paper, we study a degradation-aware network resilience strategy for QKD co-existence with classical data communication. The simulation verifies that the *SKR* can be improved by *37.6%* with a *1:5* resilient configuration of QKD channels, and *93.5%* with a proposed synergistic resilience strategy.

II. Resilience of QKD for Co-existence with Classical Data Communications

Since the introduction of WDM technology, the optical transmission system has experienced the development of larger capacity with more refined division of wavelength channels. To guarantee the quality of experience in user network, the standardized optical transport network (OTN) system provides flexible service units and complete service protection mechanism for possible link failures and recover the transmission performance in time. With quantum channels introduced into commercial optical fibers for keys negotiation, possible link failures can also interrupt the key generation. At the same time, the weak characteristics of quantum signals making them more susceptible to noise interference in addition to interruptions, resulting in fluctuations in key rates and indirectly degrading user services' security. In order to alleviate the service degradation, resilience strategies can be deployed with additional equipment to support the degradation recovery. The linear growth of SKR can be achieved by easily superimposing the QKD system over the optical links, while it also brings higher cost of QKD transceivers. In this paper, we intend to improve the yield of a single QKD system under a co-existence network, i.e., SKR, through the network resilience strategy.

A. QKD Service Degradation and Cross-layer Resilience for Coexistence with Classical Communications

Different from the classical-oriented optical network, the QKD system is expected to continuously generate keys once it was deployed. Thus, to maximize the SKR without interference of classical signals, QKD devices are conventionally settled in continuous working conditions based on dark fiber. However, with the expansion of the scenarios for coexistence of QKD and classical data communication, it is necessary to design resilience strategies against the existing nonlinear noise interference. As shown in Fig. 1(a), the networking architecture for QKD basically needs the QKD modules constituting the quantum layer, which is responsible for key generation by using QKD protocols. Then, the function of a key manager (KM) is to receive and manage keys generated by QKD modules and QKD links, relay the keys, and supply the keys to cryptographic applications. To ensure the operation and management of QKD networking, controlling and management functions are also needed. Under the co-existence scenario of QKD and classical data communications, the classical and quantum communications can be both carried in the optical network.

However, when the two kinds of communication coexist in the optical network, problems including transmission noise interference, switching resource competition, and increased controlling and management complexity, etc., will inevitably arise. In this paper, we focus on the QKD service degradation problem under the co-existence scenario. As shown in Fig. 1(b), the dynamics of classical data communication channel allocation will have varying degrees of impact on QKD communication performance, which can be referred from the nonlinear spectral characteristics of Raman scattering. In a dense WDM (DWDM) system with 100GHz channel spacing, the power spectrum of Raman scattering exhibits smooth characteristics and can cover the entire wavelength band. When multiple data channels are launched, the power magnitude of the noise interference can be superimposed, and the key generation of the QKD channel can be disabled.

Since QKD is mostly implemented through optical systems, it can refer to the protection methods of classical-oriented OTN. But the difference is that the pre-setting of additional QKD systems can only achieve a linear increase in the SKR performance of the link, which is capable to support resilience with a higher investment. Considering the process of key supply, QKD networking requires the quantum layer and the key management layer to process the keys at different stages separately, so the key supply process includes point-to-point QKD modules' key supply to KM, and end-to-end KM's key supply to user applications. Thus, we consider that the resilience of QKD needs to be considered separately at the quantum layer and the key management layer. In terms of the quantum layer, by adding available QKD modules (e.g., QKD receivers in most cases) at nodes, it can be available for flexible channel allocation strategies. In the key management layer, it is possible to realize the flexible configuration of the key stream, such as presetting an additional end-to-end key relay route, and then select a better relay route when the working key relay route fails or degrades.

B. *Adaptive Cross-layer Resource Allocation Strategy to Support QKD Resilience*

Above all, the network for QKD needs to build a resilience strategy to ensure the stable supply of keys, which can be especially significant for QKD service degradation under the co-existence with classical data communications. To guarantee the stable key supply through resilience, some improvement can be made for QKD operations. It mainly includes providing multiple QKD links for dynamic channel configuration, and realize the SKR adjustment through optimized allocation of key relay routes for end-to-end user services. From the perspective of classical communication, the resource and wavelength allocation (RWA) strategy of classical data traffic also has direct influences on the noise interference of quantum channels. Therefore, appropriate resource allocation adjustments for classical channels will also have positive significance for the resilience of QKD. This would require that the network control and management functions be capable to adjust the resource allocation for both services over the optical network.

Based on the above considerations, in this paper, we consider the adaptive QKD strategies to support the resilience for end-to-end QKD services based on 1: N QKD module configurations, which will require N additional QKD receivers on the basis of a single QKD system to enable the channel allocation for resilience. As shown in Fig. 1(c), based on the tunable QKD transmitter, *N* QKD receivers are added to QKD link A-B. For each data service request arrival, the classical services are allocated with its default channel allocation strategy (e.g., first-fit (FF) algorithm), and then the control and management functions on the QKD side perform resilience operations on the quantum layer and the key management layer, respectively. Firstly, the optimal channel is selected at the quantum layer according to the SKR or quantum bit error rate (QBER) feedback with KM, and then the controller dynamically selects the optimal end-to-end key relay route to realize end-to-end QKD service under the premise of optimizing the SKR of the point-to-point QKD systems at the quantum layer. For the degradation problem in the coexistence scenario, it is expected to improve the end-to-end SKR level as much as possible through resilience strategies.

III. Degradation-aware 1: N QKD (*DS-QKD*) Service Resilience Strategy

In this section, we propose a degradation-aware 1: N QKD (*DS-QKD*) resilience strategy to improve the SKR under service degradation in the scenario of co-existence with classical data communication. The pseudocode of *DS-QKD* service resilience strategy is shown in Table. 1. By setting N additional QKD receivers in advance to enable adaptive QKD channel configuration, channel switching can be realized in the case of QKD service degradation. When the SKR of working channel drops down, the network control and management function adjusts the wavelength channel of the QKD system transmitting devices to the higher priority channel with a higher SKR, and it is possible to restore the SKR without affecting the expected value for the key updating period.

TABLE I. The Pesudocode of Degradation-aware 1: N QKD (*DS-QKD*) Service Resilience Strategy

***DS-QKD* Service Resilience Strategy**

Input: $G(V,E,W)$, $R(S_r,D_r,B_r)$, $Q_{i,j}(S_i,D_j,\Lambda_{i,j},K_\lambda)$.
Output: F_R, k_R, routing and channel allocation for each classical request, updated network status.

Initialize $F_R \leftarrow \emptyset$;
for each classical data service $r(s_r,d_r,b_r)$ in $R(S_r,D_r,B_r)$
  K-shortest-path (KSP) algorithm for the RWA of $r(s_r,d_r,b_r)$, store the result in $p_r(s_r,d_r,k_r)$ with k_r initialized as ∞;
  find the set of wavelength channels Λ_c available for the classical service with first-fit algorithm;
  if $|\Lambda_c| \geq b_r$
    set $f_r \leftarrow true$;
    for each link (s_i,d_j) in $p_r(s_r,d_r,k_r)$
      obtain the quantum channels with their wavelengths as the set $\Lambda_q(\lambda_i,k_i)$, where $k_i=0$;
      for each wavelength channels λ_i in Λ_q
        for each wavelength channels λ_c in Λ_c
          calculate the crosstalk photon numbers $p_{i,c}$ with fronthaul or backhaul Raman scattering interference;
          calculate $p_i \leftarrow p_i + p_{i,c}$;
        end for
        estimate the SKR k_i of λ_i with p_i;
      end for
      configure the QKD channel of link (s_i,d_j) to λ_i with the max k_i;
      if $k_i \leq k_r$
        replace k_r with k_i;
      end if
    end for
  else
    set $f_r \leftarrow false$;
  end if
end for
calculate $k_R \leftarrow \sum_R k_r/|R|$
return the F_R, k_R, and updated network status.

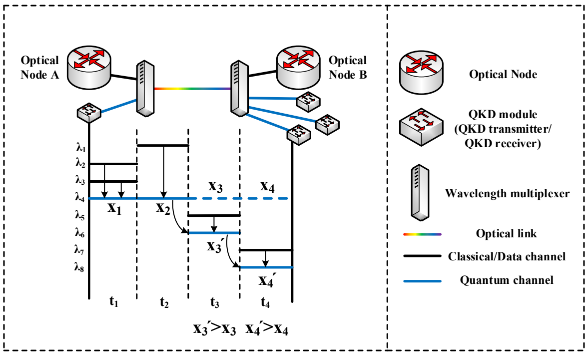

Fig. 2. *DS-QKD* strategy to support QKD resilience

As shown in Fig. 2, adopting *DS-QKD* service resilience strategy can alleviate the QKD service degradation problem caused by classical data channels' noise interference. By sampling the noise spectrum fixedly according to the channel distribution, it can be enabled with evaluating the noise photon level of the available quantum channels when classical data services arrive, and select the quantum channel with the best noise level for quantum state transmission to optimize the network SKR. If the network control and management functions can be capable to orchestrate the classical and quantum resource allocation strategies, when there are multiple optional channels for classical communication, the average photon number level of the link when different data channels are enabled can be traversed, and the channel with the lowest noise interference would be selected to launch classical data services, thus to better support the QKD resilience. According to the services distribution, the SKR decreasing by the interaction between the two can be dynamically optimized.

IV. Simulation Results

Based on the proposed QKD survivability strategy, we conducted a simulation to verify the effectiveness of the strategy in 14-node NSFNet and 24-node USNet backbone topologies with 100GHz channel spacing in each optical link. The simulation was implemented based on Java 1.8, and the decoy state-based point-to-point BB84 protocol rate calculation method was deployed to evaluate the SKR of point-to-point QKD systems as specified in Eq. (1) [10]. The parameter adopted are shown in Table. 2. Numerical values of

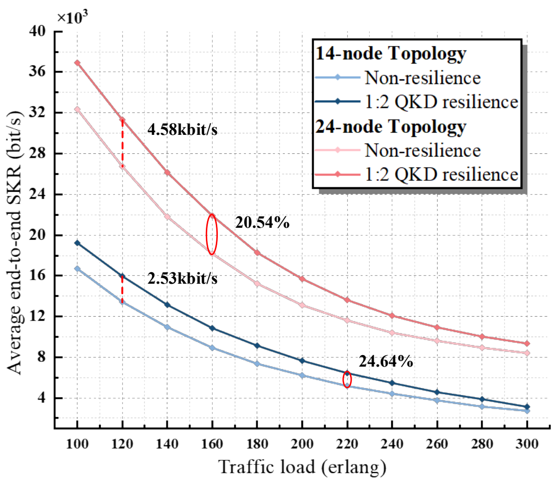

Fig. 3. Performance comparison between non-resilience and 1:2 QKD resilient configuration

Raman scattering with different channel settings are referring to the experimental analysis in [9]. Considering the limitation of SKR under backbone network with an average distance of 1000km, we proportionally reduce the distance of each link under this topology to the 10^{-2} of original distance to simulate the performance with a metropolitan area network scale, which indeed will not affect relationship between the crosstalk photon number and channel distribution. The number of classical data services is default by 10^6. In addition, considering that the throughput of QKD public channel is usually at a level of Mbps, we default a serial transmission style for integration of classical communication of QKD and data communication, and the specific transmission strategy adopted and the synchronization strategy between QKD public channel and quantum channel are ignored. In the following comparison, we simulated the average end-to-end SKR that could be obtained for classical data services.

$$R_{i,j} \geq Q_1(1 - h(e_1)) - fQ_\mu h(E_\mu), \qquad (1)$$

TABLE II. Parameter Setting of Point-to-point QKD Systems

Parameters of simulated point-to-point QKD systems	
Parameter	***Value***
Average number of photons per signal pulse, μ	0.48
Phase-distortion error probability, e_d	0.015
Quantum efficiency of detectors, η_d	0.2
Channel loss coefficient, α	0.046km^{-1}
Receiver dark count rate, γ_{dc}	1E-7ns^{-1}
Time gate interval, T_d	100ps
Bandwidth guardband, *Δ*	200GHz
QKD receiver frequency, f_s	2Mhz

As shown in Fig. 3, comparing the performance of the proposed QKD resilience strategy and static channels configuration in terms of SKR, under different traffic load, the proposed *DS-QKD* method can improve the SKR. The maximum improvement is about *24.64%* and *2.53kbit/s* under 14-node topology. As the time-intensiveness of the classical communication increases, that is, the traffic load increases, the optimization effect gradually decreases. We consider that this is because in the case of heavier traffic load, the fixed channel setting makes the number of crosstalk photons of each quantum channel close to the same, which narrows the difference among the final SKR upper limit of multiple QKD channels. Therefore, the optimization effect of *DS-QKD* in the case of intensive traffic will be significantly weakened.

Therefore, we try to linearly add more quantum channels to improve the SKR optimization under heavier traffic loads, and the added QKD wavelength channels are randomly selected. We simulated the relationship between SKR and

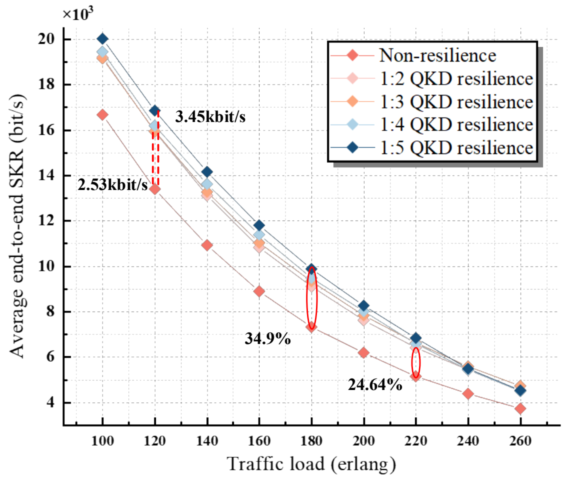

Fig. 4. Performance comparison between non-resilience and 1:N QKD resilient configuration with different values of *N*

traffic load under the conditions of *N=2, 3, 4,* and *5*, as shown in Fig. 4. In the case of *120* erlangs traffic load, adding 4 additional QKD channels can increase *SKR* by about *25.8%* (i.e., *3.45* kbit/s by maximum). In the case of a traffic load of *140* erlangs, QKD resilience scheme with *N=5* increases *SKR* by about *7.9%* (i.e. *1.04* kbps) compared to N=2 situation. It can be seen that the additional QKD link can further enhance the resilience of QKD channels configuration and improve end-to-end *SKR* indirectly. However, it can also be seen that more QKD transceivers do not bring about a linear increase in *SKR*. There exists a nonlinear relationship between the end-to-end *SKR* increase and the number of added QKD channels, which also has relevance with the wavelength of the added channel.

In the above process of adding QKD wavelength channels to enhance resilience, we found that different combination of channels also has a significant impact on the effect of SKR improvement. Therefore, we compare the end-to-end SKR between compact channel setting and adjacent channels for QKD resilience. A uniformly spaced channel setting is deployed to simulate the relationship between *SKR* and traffic load, as shown in Fig. 5. The fixed channel is set to λ_3. It is interesting that when the channels are selected as $\{\lambda_0, \lambda_1, \lambda_2, \lambda_3\}$, the average end-to-end *SKR* has a general decline in performance. When wavelength channels $\{\lambda_{10}, \lambda_{15}, \lambda_{20}, \lambda_{25}\}$ are selected for the quantum channel configuration at equal intervals, the *SKR* has a significant increase. We consider that this can be related to the spectral characteristics of Raman scattering, that is, there is several low-loss windows of the Raman scattering power spectrum, which are usually distributed in the adjacent wavelengths range of the classical data channels. Thus, the compact style of quantum channel settings increases the average number of crosstalk photons generated by each classical data channel, so the average *SKR* of the network has a performance degradation problem. When $\{\lambda_3, \lambda_{13}, \lambda_{23}, \lambda_{33}\}$ are selected with a larger wavelength interval, the average end-to-end SKR continues to increase. Thus, it can be concluded that a reasonable equidistant QKD channel configuration can enable the low-loss window area for classical data services and optimize the average end-to-end SKR of the co-existence network. When the traffic load is *100* erlangs, the SKR can be improved by *37.6%* (i.e., *5.35* kbps) with a uniformly spaced

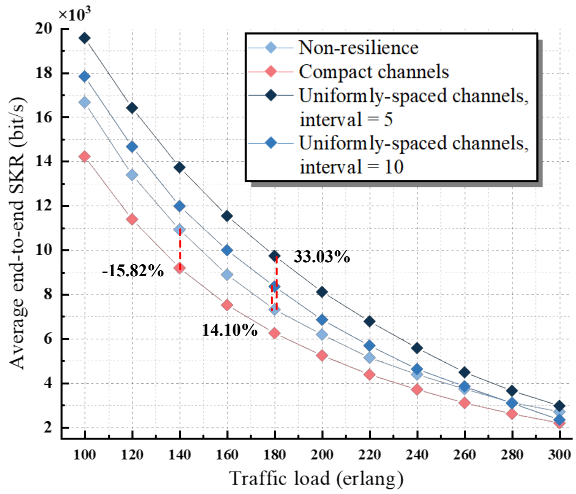

Fig. 5. Performance comparison between non-resilience scheme QKD resilience configuration with compact channels or uniformly-spaced channels

channels of interval equals to 10 wavelengths comparing to the compact channel strategy.

Finally, we simulated the effect of classical resource allocation strategy on QKD resilience performance. In conclusion, adopting coordinated classical resource allocation scheme has a boosting effect on the resilience performance of the quantum channels. With an adaptive data channel allocation strategy, significantly higher SKR can be achieved as shown in Fig. 6. The classical data channel is allocated to the wavelength with the best performance of the quantum channels during the path search iteration to optimize the end-to-end secret-key yield of the entire network. For the classical communication, we adopt a crosstalk photon equalization strategy for classical channel allocation, and the optimization effect becomes more and more significant as the traffic load increases. Under the traffic load of *260* erlangs, the *SKR* optimization rate reaches *96.38%* (i.e., *4.37* kbps) compared with the non-resilience QKD channels configuration. In the case of worse channel conditions with large traffic load scenarios, the adaptive resilience strategy can make SKR increase exponentially, which has positive significance for the

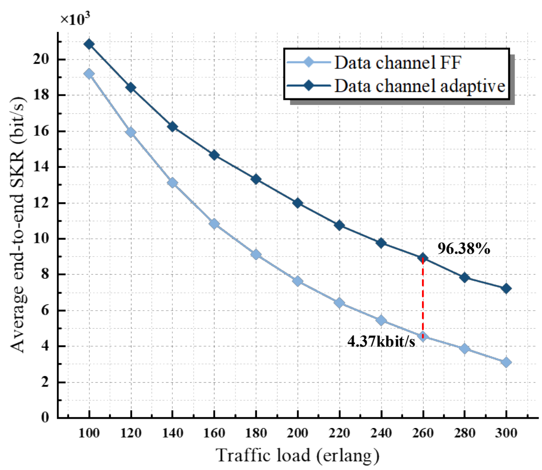

Fig. 6. Performance comparison between QKD resilience configuration scheme with FF strategy and synergistic resilience of classical communication

application and integration of QKD in large-scale classical communication-oriented optical networks.

V. Conclusion

In this paper, we discuss the resilience scheme under the co-existence network of QKD and classical data communication, and propose a cross-layer QKD resilience scheme based on degradation awareness. It is verified that the proposed *DS-QKD* strategy can improve *SKR* about *37.6%* under the resilient configuration with 1:5 additional QKD transceivers in quantum layer, the primary proposed adaptive resilience scheme can increase SKR by about *96.4%*, and can increase SKR multiples under heavier traffic load conditions.

References

[1] C. O. Klingenberg, M. Borges, and J. Antunes Jr, “Industry 4.0 as a data-driven paradigm: a systematic literature review on technologies,” J. Manuf. Technol. Manag., vol. 32, pp. 570-592, Mar 2021.

[2] V. Bajaj, F. Buchali, M. Chagnon, S. Wahls, and V. Aref, “Single-channel 1.61 Tb/s optical coherent transmission enabled by neural network-based digital pre-distortion,” In 2020 European Conference on Optical Communications (ECOC), pp. 1-4, December 2020.

[3] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and Zhang, J. “KaaS: Key as a service over quantum key distribution integrated optical networks,” IEEE Comm. Magazine, vol. 57, pp. 152-159, Mar 2019.

[4] M. Sasaki, et al., “Field test of quantum key distribution in the Tokyo QKD Network,” Opt. Express, vol. 19, pp. 10387-10409, May 2011.

[5] S. K. Liao, et al., “Satellite-to-ground quantum key distribution,” Nature, vol. 549, pp. 43-47, Aug 2017.

[6] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, “Quantum key distribution secured optical networks: A survey,” IEEE Open Journal of the Communications Society, vol. 2, pp. 2049-2083, Aug 2021.

[7] F. Beutel, H. Gehring, M. A. Wolff, C. Schuck, and W. Pernice, “Detector-integrated on-chip QKD receiver for GHz clock rates,” npj Quantum Information, vol. 7, pp. 40, Feb 2021.

[8] Y. Mao, et al., “Integrating quantum key distribution with classical communications in backbone fiber network,” Opt. Express, vol. 26, pp. 6010-6020, Feb 2018.

[9] C. Cai, Y. Sun, and Y. Ji, “Simultaneous long-distance transmission of discrete-variable quantum key distribution and classical optical communication,” IEEE Transactions on Communications, vol. 69, pp. 3222-3234, Feb 2021.

[10] I. George, J. Lin, and N. Lütkenhaus, “Numerical calculations of the finite key rate for general quantum key distribution protocols,” Physical Review Research, vol. 3, pp. 013274, Mar 2021.