Power-scheduled Routing Strategy for Quantum Key Distribution over Classical Optical Networks

Yuhang Liu
State Key Lab of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications
Beijing, 100876 China
yuhangliu@bupt.edu.cn

Xiaosong Yu
State Key Lab of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications
Beijing, 100876 China
xiaosongyu@bupt.edu.cn

Yongli Zhao
State Key Lab of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications
Beijing, 100876 China
yonglizhao@bupt.edu.cn

Avishek Nag
School of Computer Science, University College Dublin, Belfield, Dublin 4, D04 V1W8
Ireland
avishek.nag@ucd.ie

***Abstract*—In this work, we study a power-scheduled routing strategy for quantum key distribution (QKD) over classical optical networks. The average secret key rate can be improved by 59.4% and 152.8% at maximum with the proposed routing algorithms of end-to-end and point-to-point optimization, respectively.**

Keywords—Quantum key distribution (QKD), optical network, power-scheduled, routing

I. INTRODUCTION

With the continuous growth in information traffic, high capacity and flexibility become the focus of optical network development [1]. Quantum communication, also based on photonic technology, is making an impact on classical optical networks regarding communication capacity, security, and energy consumption [2]. At the same time, quantum computing, exemplified by quantum processors, is posing a threat to the security of encryption methods based on computational complexity in classical optical networks, and may become an important vulnerability of communication services. As the world's primary information and communication infrastructure, the security of high-capacity data communication has undoubtedly garnered increased attention.

Quantum key distribution (QKD) completes the post-selection-based key agreement process through quantum and classical channels, outputting long-term secure keys for data encryption. QKD is typically set up as a point-to-point (P2P) system, constructing a QKD network via back-to-back key relay to supply end-to-end (E2E) keys [3]. The key supply service can be decoupled from the underlying infrastructure through management and control technologies [4], and then the keys are provided for communication nodes with cryptographic applications. However, to ultimately serve multi-point to multi-point encrypted user communications, considering factors such as key-redistribution security and equipment deployment costs, QKD needs further integration with existing optical communication infrastructure. The current approach is using dark fiber resources to carry QKD communication, reserving channels independently for continuous key generation. But with limited optical fiber resources, this incurs high-cost investment. Another method is integrating QKD systems with classical optical communication systems link-by-link, but noise greatly limits the final key rate. Therefore, the incompatibility between QKD and optical communication systems restricts the practical application of QKD in large-scale networks.

Given the high optical loss in the O-band, an ideal deployment approach is to co-propagate classical and quantum signals in the C-band. However, dense channel distribution leads to more severe noise effects [5]. Since the power level of classical signals far exceeds that of quantum signals, the classical signals have an inhibitory effect on quantum signal reception, including four-wave mixing (FWM), spontaneous Raman scattering (SRS), etc. At the switching nodes, there are insertion loss and power crosstalk between adjacent channels. To overcome noise interference during co-propagation of classical and quantum channels, researchers have explored methods including adopting improved fiber structures, configuring auxiliary filters, and optimizing channel allocation to weaken the suppression of classical channels on quantum channels. Regarding fiber structure improvement, multi-core optical fibers and hollow-core optical fibers have been proposed to reduce co-propagation interference [6]. Based on cascaded amplifier and filter configurations, optimal channel assignment models have been discussed to reduce noise of FWM, SRS and inter-channel crosstalk [5].

The system demonstrations on co-propagation can support encrypted communication above a data scale of 100G by the time of writing. Researches have conducted substantial analysis and improvement on P2P co-propagation systems, forming performance-optimized co-propagation links through predetermined fibers and channel deployment. However, interference of SRS has been shown to still not be completely rejected at the receiver end, making it challenging for C-band co-propagation systems application in large-scale network with E2E services. In [6], a DWDM system for co-propagation of classical and quantum signals was demonstrated, where the noise intensity of SRS depends on the wavelength spacing between the classical and quantum channels, as well as the power level of the classical signals. There is a deficiency in network-layer algorithms that support the optimal utilization of channel resources in dynamic service scenarios.

In this work, we introduce an adaptive routing strategy based on power scheduling to facilitate the transition from classical optical networks to compatible large-scale networks that support QKD. Building upon the routing methods for transparent transmission in existing optical networks for classical communication, this work discusses the power-scheduled adaptive routing strategies based on both E2E path and P2P link optimization. While P2P optimization incurs greater monitoring and control overhead, it significantly

This work was supported by NSFC project (61971068, 62150032, U22B2026), Innovation Program for Quantum Science and Technology (2021ZD0300704), the Funds for Creative Research Groups of China (62021005), the Fundamental Research Funds for the Central Universities (2023PY08), and BUPT Excellent Ph.D. Students Foundation under Grant CX2023140.

enhances the average secret key rate (SKR). Within a 38-node network topology, E2E-based power scheduling algorithm improves average SKR by 59.4%, whereas the P2P-based algorithm further increases this enhancement to 152.8%.

II. Architecture of Optical Networks for Coexistence of Classical Communication and QKD

QKD networking based on optical fiber communication infrastructure to realize P2P QKD systems will become a long-term reality. The compatibility of classical and quantum communication will be manifested in the physical coexistence, logical co-management, which requires sharing of physical and logical resources. As depicted in Fig. 1, the optical network architecture supporting QKD adds quantum plane and key management key management plane over data plane to facilitate the generation and provisioning of secret keys. Within the data plane, the optical cross-connect (OXC) is responsible for the signal exchanging, while in the quantum plane, QKD modules conduct quantum state transmission and agreement through both classical and quantum channels. The key management plane processes the keys generated by the quantum layer, performing tasks such as formatting and synchronization. The key supply rate (KSR), from generation to provisioning, is ultimately determined by the key relay routing in the key management plane. For instance, if SKR between QKD nodes A and B is x Mbit/s, and between nodes B and E is y Mbit/s, the KSR based on key relay for a key request initiated between nodes A and E will be x Mbit/s when $x \leq y$. In the control plane, to ensure security, the software-defined networking (SDN) controllers serving classical data communications and QKD will operate in isolation and communicate through interworking interfaces. At the application plane, the keys supplied by key managers are used for encryption in accordance with the cryptographic schemes employed by the classical communication system.

In a WDM based optical network for coexistence of classical communication and QKD, the classical communication consists of data communication in data plane, measurement communication supporting QKD plane, KM intercommunication in key management plane, and controlling communications. These classical communications can be realized on classical channels through time-division multiplexing and other techniques [7]. From the physical coexistence point of view, researches have analyzed the phenomena and nature of co-propagation, and refined models of noise effects including SRS to guide actual channel deployment. In [5], it proposed a joint optimized channel allocation method to suppress the FWM and SRS noise, where quantum channels and classical channels were interleaved with each other. These works mainly optimize P2P communication systems in a static manner, while practical network services require dynamic E2E configuration across heterogeneous classical and quantum systems. The inability of static configurations to adapt to varying noise presents a major challenge. From the logical co-management point of view, the network for co-existence of classical communication and QKD includes heterogenous routing methods for classical data communication and QKD separately. The former mainly focuses on ensuring E2E signal reachability, while the latter tends to ensure stable P2P key generation and E2E key supply, respectively. When classical data communication and QKD coexist in the optical network, the routing strategy for classical data communication can affect QKD due to noise effects.

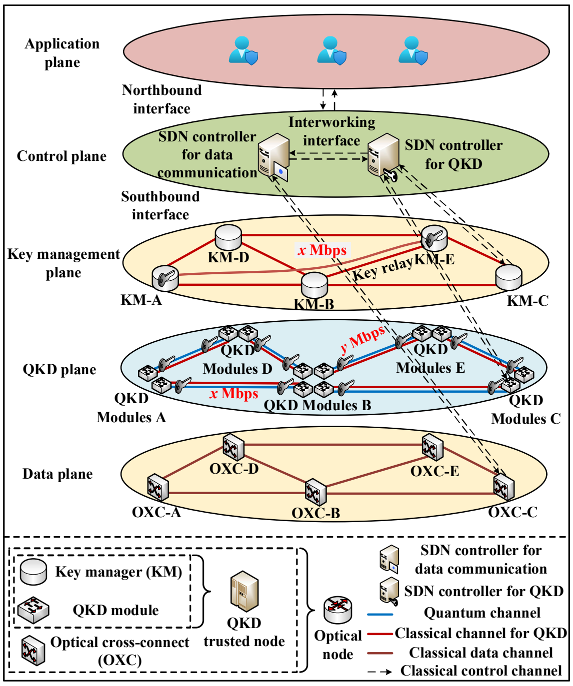

Fig. 1. An optical network architecture for coexistence of classical data communication and QKD.

A. Impact of Classical Communication Routing on QKD

Based on different routing objectives, the routing strategies for classical data communication can impact the performance of QKD systems to varying degrees. During the co-propagation of classical and quantum signals, the classical signals can reduce the valid photon count with QKD receiver, subsequently decreasing the SKR. According to the fitting formula of SRS power spectrum, the scattering effect between classical and quantum signals mainly depends on (1) the transmission power of the classical signal, (2) the wavelength spacing between the classical and quantum channels, and (3) the co-propagation distance. Typically, QKD is supposed to be deployed in a P2P form in optical networks. To conclude, classical signals mainly impact quantum channel performance through two primary factors - power level and routing strategy (i.e., the routing and wavelength assignment). Based on SDN controller and operability between optical devices, it is promising to achieve adaptive adjustment of the above factors for better QKD performance.

B. Classical-oriented Adaptive Routing Strategy

The coexistence of classical data communication and QKD can be supported by incorporating dynamic power scheduling to achieve better QKD performance. Within an all-optical network, OXCs are capable of wavelength switching and signal power adjustment, where the SDN controller plays a pivotal role in continuously monitoring the network conditions and adjusting parameters to optimize performance. By transmitting classical signals at the minimum necessary power, the network minimizes SRS interference with quantum channels and leverages routing reconfigurations to respond to the dynamic nature of network traffic. Such classical-oriented adaptive routing strategy, particularly the agile modulation of classical signal power, is instrumental in the objective improvement of QKD performance.

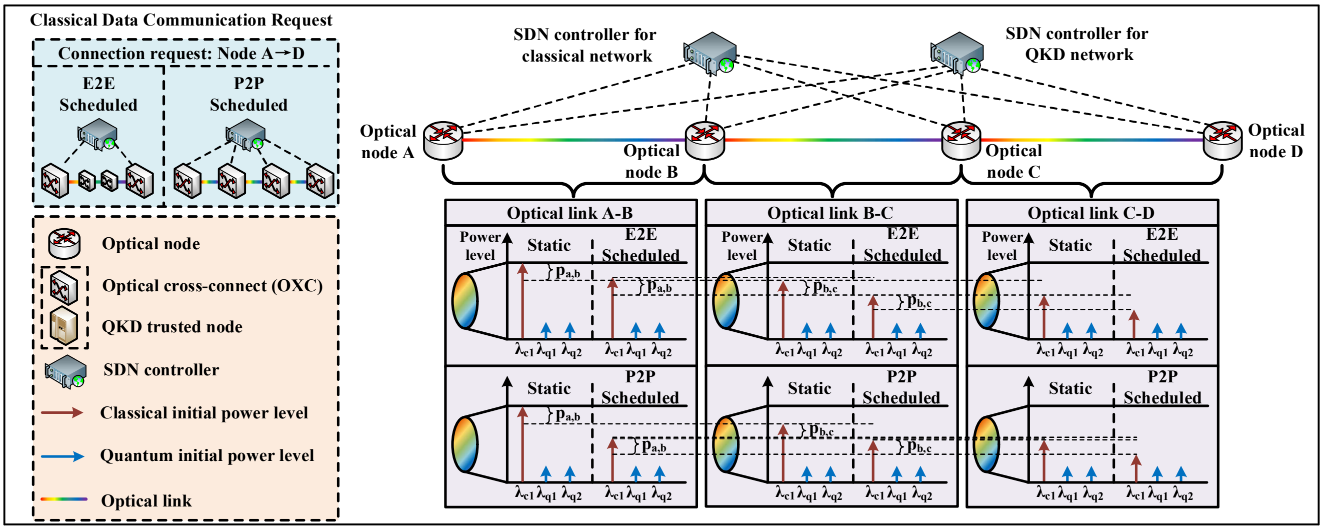

Fig. 2. P2P and E2E power-scheduled routing strategy for QKD over optical path.

As illustrated in Fig. 2, the power level of static configuration for classical optical signal transmission are typically set at a fixed output to ensure signal integrity, which do not account for QKD performance. To mitigate the noise impact on QKD, we propose two power-scheduled routing strategies: an E2E, service-oriented power-scheduled routing strategy, and a P2P, physical link-based power-scheduled routing strategy, the latter often resulting in increased monitoring and control overhead. Acknowledging the additional overhead and optical losses incurred by power monitoring and adjustment, we also consider partially P2P power scheduling into the overall strategy, allowing for power adjustments at specific nodes along the optical path. It is evident that on a four-node optical path, the E2E power-scheduled routing strategy maintains higher power levels at the initial links to meet receiver sensitivity requirements, yet reduces the overall power level, yielding optimization benefits. Conversely, the P2P power-scheduled routing strategy adaptively adjusts the power of the optical signal at each hop, further reducing the power level of classical signals, resulting in enhanced optimization for QKD.

III. Power-Scheduled Routing Algorithm For QKD over Classical Optical Networks

In this section, we propose the power-scheduled routing algorithm for QKD over classical optical network (PS-QKD). PS-QKD conducts power scheduling upon routing outcomes derived from the first-fit (FF) algorithm. It executes power adjustment after traversing the agreed number of hops σ to segment the candidate path. In this context, P2P power scheduling corresponds to $\sigma = 1$, indicating power modulation at every hop, whereas E2E scheduling sets σ to the length of the candidate length, suggesting a singular power modification at the transmitter end. For partial P2P power scheduling, σ remains an adjustable parameter, which is chosen to balance the trade-off between control and management overhead and power optimization efficiency along the optical path. This granular approach allows for the fine-tuning of the power scheduling to the specific requirements of network traffic and control complexity. Based on PS-QKD, the scheduled routing result for each connection request can reduce the average power on each link, thereby achieving the desired average SKR.

TABLE I. The Pseudocode of PS-QKD Routing Algorithm

PS-QKD Routing Algorithm

Input: $G(V,E,W)$, $R(S_r, D_r, B_r)$, $Q_{i,j}(S_i, D_j, \Lambda_{i,j}, K_\lambda)$, insertion loss η_{il} of each node, channel loss coefficient α, segmentation hop σ.

Output: F_R, k_R, scheduled routing result π_R, wavelength assignment for each classical request, and updated network status.

1 **Initialize** $F_R \leftarrow \emptyset$;
2 **for** each classical data service $r(s_r, d_r, b_r)$ in $R(S_r, D_r, B_r)$
3 FF algorithm for $r(s_r, d_r, b_r)$, store the result as $\pi_f(s_r, d_r)$;
4 **initialize** $\pi_{sr}(\pi_{ri}, p_{ri}) \leftarrow \emptyset, f_r \leftarrow false, p_r \leftarrow 0$;
5 find the set of common wavelength channels Λ_c available across $\pi_f(s_r, d_r)$ with FF algorithm;
6 **if** $|\Lambda_c| \geq b_r$
7 set $f_r \leftarrow true$;
8 **for** each link (s_i, d_j) in $\pi_f(s_r, d_r)$
9 set power budget for the link $p_{i,j} \leftarrow p_{i,j} + \alpha \cdot l_{i,j}$;
10 $p_{i,j} \leftarrow p_{i,j} + \eta_{il}, p_r \leftarrow p_r + p_{i,j}$;
11 add (s_i, d_j) to the scheduled path segment $\pi_r(s_i, d_j)$;
12 **if** $|\pi_r(s_i, d_j)| \geq \sigma$
13 $p_r \leftarrow p_r + p_m$;
add (π_r, p_r) to the scheduled path $\pi_{sr}(\pi_{ri}, p_{ri})$;
14 **initialize** $\pi_r(s_r, d_r) \leftarrow \emptyset, p_r \leftarrow 0$;
15 **end if**
16 **end for**
17 add $\pi_{sr}(\pi_{ri}, p_{ri})$ to the scheduled routing result π_R;
18 **else**
19 set $f_r \leftarrow false$;
20 **end if**
21 **end for**
22 **return** the F_R, π_R, and updated network status.

As indicated in Table I, for each request of data service $r(s_r, d_r, b_r)$, line 3 adopts the FF algorithm to select the candidate optical path with available wavelength channels for the service carrying. In line 4-5, it initializes the routing result $\pi_{sr}(\pi_{ri}, p_{ri})$ and flag of service availability f_r, where π_{ri} represents each power scheduling segment with the scheduled transmit power p_{ri}. And f_r is true when the service is capable of being carried with the candidate optical path. According to the wavelength consistency for classical data communication, Λ_c can be filtered out. In lines 6-7, PS-QKD first judges that whether the available wavelength channels are sufficient for the request, where f_r is set to true when the candidate path is capable. Lines 8-16 calculate the power budget of each routing segment based on the insertion loss over traversed nodes and the propagation loss of traversed links (s_i, d_j), where $p_{i,j}$ indicates the total power loss, measured in decibels, during optical switching and co-propagation. For optical switching, η_{il} represents the insertion loss across each OXC with its optical components. For co-propagation, the optical fiber loss coefficient, denoted as α, is multiplied by the length of each optical link $l_{i,j}$ to calculate the total propagation loss. When the number of elements in the routing segment $|\pi_r(s_i, d_j)|$ equals to σ, a power margin p_m is factored into the power budget to ensure the power scheduling is robust and accounts for all potential attenuations. Then, the routing segment result is added to the complete routing result $\pi_{sr}(\pi_{ri}, p_{ri})$, where (π_r, p_r) is initialized for further scheduling segment. Finally, the union of these segmented routing results constitutes the complete routing result for each request with PS-QKD, which is delivered to the network control and management layer for configuration and service provisioning. Line 17 documents the routing outcome for each request, aggregating these into the comprehensive set of routing results denoted by π_R.

IV. Simulation Results

Based on the strategy and pseudocode of PS-QKD as illustrated in Section III, we simulated and analyzed its feasibility and performance in this section. We select network topologies with 6 and 38 nodes, with link distances characteristics of metropolitan scales, ranging from 20 to 60 kilometers, where the FWM effects is negligible compared to SRS in the context [8]. There are 40 wavelength channels arranged at equal intervals of 0.8nm in the C-band. The simulation is implemented based on Java 1.8. In terms of classical communication services, the arrival of services follows a Poisson distribution, and the traffic load is selected within the range of 100-300 erlangs with a step size of 20 erlangs. According to the simulation results, the average SKR for 10^6 service arrivals in the 6-node topology drops sharply. Thus, the number of service arrivals is set to 10^5. For QKD, the decoy-state discrete-variable QKD (DV-QKD) protocol is deployed by default between each pair of nodes for key agreement. The DV-QKD simulation parameters adopted for SKR calculation using Eq. (1) are shown in Table II [9]. The quantum channel is carried by the first available wavelength channel by default, while the adjacent wavelength channels are shielded to avoid the adjacent channel crosstalk noise at the QKD receiver [10].

TABLE II. Parameters Setting of DV-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	100GHz
Pulse repetition frequency, f_s	2Mhz

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

As shown in Fig. 3, we compared the average SKR of the power-fixed routing strategy for QKD (PF-QKD) and PS-QKD in 6-node and 38-node topologies. The network average SKR represents the mean value of SKR on each link during the service arrival and release, where the simulation duration is determined by the time difference between the arrival of the first classical data service and the release of the last data service. With the PF-QKD strategy, the classical optical signal power is fixed at 0dBm, while with the PS-QKD strategy, the E2E classical optical signal power budget is calculated during the routing process, so as to evaluate the feasibility of the proposed power scheduling strategy.

The trends of the curves in Fig. 3 show that PS-QKD can optimize SKR under different simulation conditions. The results exhibit an upward trend in SKR with higher traffic loads, which can be attributed to the dynamic nature of the proposed routing and power scheduling algorithms. As the traffic load increases, the frequency of service arrivals and departures intensifies. This frequent fluctuation in network activity provides more opportunities for the algorithm to dynamically adjust and optimize the optical paths and power levels for QKD improvement. Instead of static resource allocation, which could lead to inefficiencies under variable traffic loads, the proposed algorithm can actively respond to changes in traffic patterns, redistributing resources in real-time. This results in a more efficient utilization of the network's spectral resources and, paradoxically, allows for a higher average SKR despite the increased overall traffic load. Regarding the fluctuation of the improvement, we consider that it indicates the non-linear relationship between traffic load and SKR under resource allocation activities, as well as disproportionately optimization benefits for further study.

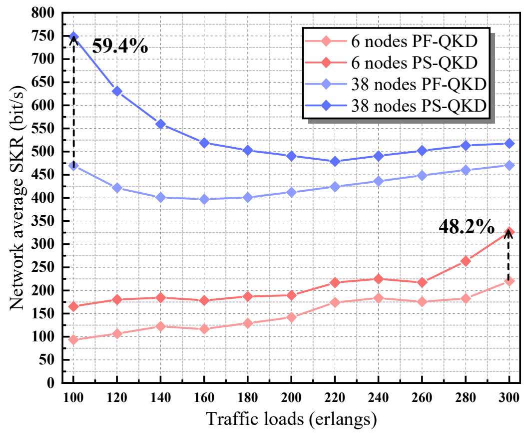

Fig. 3. Performance comparison between PF-QKD and PS-QKD under 6-node and 38-node network topologies.

Furthermore, the improvement of SKR is greater in the 38-node network topology than in the 6-node network topology under a relatively low traffic load, and performs the opposite when traffic load becomes heavier. Under the 38-node topology, the relative improvement of SKR reaches 59.4% with 100 erlangs traffic load, while the improvement is 48.2% under 6-node topology with traffic load of 300 erlangs. It indicates that the topology of network also has influence on PS-QKD optimization. More routing choices under a larger network scale leads to reduced crosstalk and potential interference when the traffic load is low, whereas it can present a more complex scenario with longer optical paths and higher average transmitting power for dynamic routing of increased traffic. Consequently, PS-QKD not only need to address only the optimal routing for QKD but also the management of classical traffic, which can lead to less improvements in SKR despite the same or higher traffic loads. Therefore, the topological complexity, indicated by the number of nodes and the nature of the interconnections between them, could be a determining factor in the performance of PS-QKD algorithm.

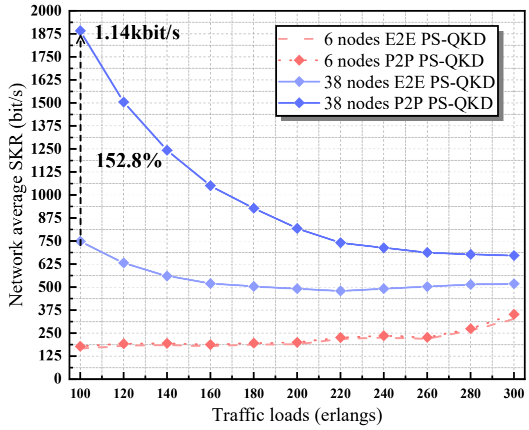

Fig. 4. Performance comparison between E2E PS-QKD and P2P PS-QKD under 6-node and 38-node network topologies.

Based on the feasibility of PS-QKD analyzed above, we further simulated and analyzed the performance impact between E2E and P2P PS-QKD, which focuses on whether the additional controlling and monitoring overhead can further enhance the optimization effect of PS-QKD. As shown in Fig. 4, enhanced P2P PS-QKD is assumed to support adjustment of classical optical signals at each intermediate node, where the transmit power can be scheduled based on the power budget of each link. It can be seen that P2P PS-QKD can significantly improve SKR in the 38-node topology, increasing it by about 1.14kbit/s under a 100 erlangs traffic load, corresponding to a relative improvement of 152.8%. However, this enhancement effect can be weakened with increased traffic load and reduced topology scale. Under the 6-node topology, the SKR obtained by P2P PS-QKD is almost identical to that of E2E PS-QKD. We consider that in small-scale topologies, the number of hops for routing calculation is relatively fixed, while wavelength channels occupancy is also relatively high. Therefore, optimiazation effects for P2P and E2E power scheduling tend to be consistent.

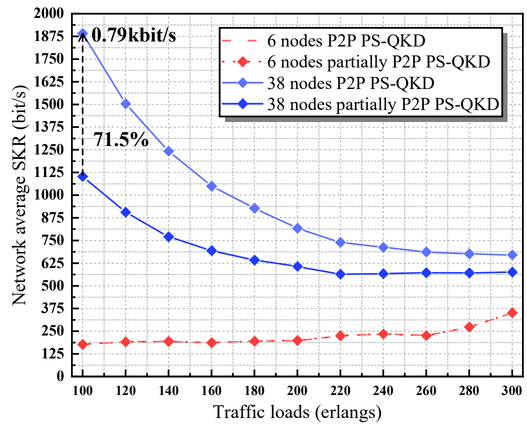

Fig. 5. Performance comparison between PS-QKD and partially P2P PS-QKD under 6-node and 38-node network topologies.

Considering the trade-off between optimization effects and overheads for optical network control and management, potentially causing pressure on actual network operations. We simulated and analyzed the performance of partially P2P PS-QKD, where the segmentation hop σ is set to 2. As shown in Fig. 5, under the 6-node topology, partially P2P PS-QKD does not achieve optimization as well, for reasons consistent with the situation in Fig. 4. Under the 38-node topology, the SKR improvement of partially P2P PS-QKD reaches 47.4%, while P2P PS-QKD improves SKR by about 0.79kbit/s over partially P2P PS-QKD with a relative improvement of 71.5%. These simulation results demonstrate that the network control and management functions can dynamically configure attributes of PS-QKD based on network traffic conditions and control and management capability.

V. Conclusion

In this study, we have discussed an adaptive routing strategy for QKD over classical optical networks, and introduced a power-scheduled routing algorithm (PS-QKD). Our results confirm that the PS-QKD algorithm can improve the average secret key rate (SKR) by 59.4% in end-to-end and 152.8% in point-to-point (P2P) optimization scenarios at maximum. We have identified that the correlation between traffic load and SKR, particularly in the context of resource allocation, along with the observed disproportionate optimization benefits, warrants deeper investigation. Furthermore, the partially P2P PS-QKD strategy demonstrates that judicious power adjustments can effectively navigate the trade-offs between control and management overheads and the efficiency of power optimization throughout the optical path, which also provides an opportunity to mitigate the impacts of varying traffic conditions and network topologies. Further work will be involved into these aspects to enhance the applicability of QKD in complex optical networks.

References

[1] 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.

[2] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, “High-dimensional quantum communication: benefits, progress, and future challenges,” Advanced Quantum Technologies, vol. 2, pp. 1900038, October 2019.

[3] X. Yu et al, “Secret-Key Provisioning with Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks,” Journal of Lightwave Technology, vol. 40, pp. 3530-3545, Feb. 2022.

[4] X. Yu et al, “Multi-path-based quasi-real-time key provisioning in quantum-key-distribution enabled optical networks (QKD-ON),” Opt. Express, vol. 29, pp. 21225-21239, Jun. 2021.

[5] J. N. Niu, Y. M. Sun, C. Cai, and Y. F. Ji, “Optimized channel allocation scheme for jointly reducing four-wave mixing and Raman scattering in the DWDM-QKD system,” Applied optics, vol. 57, pp. 7987-7996, September 2018.

[6] P. Gavignet et al, “Co-propagation of 6 Tb/s (60* 100Gb/s) DWDM & QKD channels with~ 17 dBm aggregated WDM power over 50 km Standard Single Mode Fiber,” In Optical Fiber Communication Conference, pp. Tu3H-2, Optica Publishing Group, March 2023.

[7] Y. Zhao et al, “Resource allocation in optical networks secured by quantum key distribution,” IEEE Communications Magazine, vol. 56, no. 8, pp. 130-137, August 2018.

[8] N.A. Peters et al, “Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments,” New Journal of physics, vol. 11, no. 4, pp. 045012, April 2009.

[9] 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.

[10] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, “Quantum key distribution and 1 Gbps data encryption over a single fibre,” New Journal of Physics, vol. 12, no. 6, pp. 063027, June 2010.