



Enhancing the reliability of multipath QKD over multi-band systems

Downloaded from: <https://research.chalmers.se>, 2026-04-14 13:05 UTC

Citation for the original published paper (version of record):

Ahmadian, S., Arpanaei, F., Carlos Hernandez-Hernandez, J. et al (2025). Enhancing the reliability of multipath QKD over multi-band systems. *Journal of Optical Communications and Networking*, 17(12): 1105-1116. <http://dx.doi.org/10.1364/JOCN.569098>

N.B. When citing this work, cite the original published paper.

© 2025 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, or reuse of any copyrighted component of this work in other works.

Enhancing the reliability of multipath QKD over multi-band systems

MORTEZA AHMADIAN,^{1,*} FARHAD ARPANAEI,² JUAN CARLOS HERNANDEZ-HERNANDEZ,² RUI LIN,¹ AND PAOLO MONTI¹

¹Electrical Engineering Department, Chalmers University of Technology, Gothenburg, Sweden

²Universidad Carlos III de Madrid, 28911 Leganes, Madrid, Spain

*seyedah@chalmers.se

Received 30 May 2025; revised 19 September 2025; accepted 29 September 2025; published 13 November 2025

Quantum key distribution (QKD) networks offer scalable secure communication, while efficient integration with existing optical infrastructure requires careful consideration. This paper investigates enhancing the security of multipath QKD over multi-band systems by exploring the trade-offs between multi-band separation and multipath techniques. A novel, to our knowledge, framework, incorporating blocking ratio analysis for a single and multipath QKD, is proposed, comparing bitwise product and concatenated key generation methods. Our model considers propagation delays and key pool synchronization's impact on the secret key rate (SKR). Our simulations using a U.S. long-haul network model demonstrate significant benefits of implementing QKD in alternative spectral bands. The results show substantial improvements in SKR at various span lengths in single-path scenarios. Additionally, increasing the number of quantum channels led to noticeable reductions in network blocking rates, enabling higher classical traffic loads throughout the network infrastructure. We introduce, to our knowledge, new KPIs: the blocking rate (B_{CQ}) and a comprehensive security rate (C), assessing the final key's overall secrecy. For multipath schemes, simulations reveal that concatenated multipath QKD, while exhibiting a superior blocking rate, showed 12% less compromised secrecy at 4000 km (32% to 20%), compared to less than 10% for bitwise product multipath QKD under the same conditions. These findings provide valuable insights into designing efficient and secure quantum-enhanced optical networks, highlighting the complex interplay between security and efficiency in multipath QKD architectures.

Published by Optica Publishing Group under the terms of the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/). Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

<https://doi.org/10.1364/JOCN.569098>

1. INTRODUCTION

QKD systems leverage the principles of quantum mechanics to ensure unconditionally secure communication, as any attempt to eavesdrop disturbs the quantum state and can be detected [1]. QKD offers resilience against potential quantum computing attacks, improving sensitive information protection. It ensures that the keys exchanged are authentic and intact, making it suitable for critical applications such as financial transactions and secure government communications [2,3].

A point-to-point QKD connection involves a dedicated communication channel between two parties, such as a single optical fiber, used exclusively for key exchange. Although this setup is straightforward and highly secure, its scalability is limited since a new channel must be established for each additional connection. To overcome this limitation, QKD networks have been developed, interconnecting multiple nodes through various communication channels. These networks enable QKD in larger, decentralized systems, supporting

multiple users and applications such as network-based financial transactions and critical infrastructure protection [4].

While QKD networks improve scalability and flexibility, widespread deployment remains challenging due to the high cost of laying new optical fibers dedicated to quantum channels. To address this, integrating QKD with existing optical backbone infrastructure has emerged as a practical solution, allowing QKD to operate alongside classical communication. This approach enables secure, high-speed data transmission for applications such as cloud services, secure data centers, and inter-city communication links [5]. However, integrating QKD with classical optical networks introduces challenges. Nonlinear effects in optical fibers, such as four-wave mixing, Raman scattering, and cross-phase modulation, can degrade quantum signals, causing noise and errors in key generation. These effects pose significant obstacles to ensuring secure QKD performance when sharing fiber channels with classical data [6].

One solution to tackle these nonlinearities is to take advantage of the channel spacing between classical and quantum channels. This allows the simultaneous transmission of multiple signals within different frequencies over the same optical fiber. This method not only maximizes the utilization of the existing infrastructure but also enables better spectral efficiency and scalability, reducing the need for additional physical resources or fibers [7]. However, suppose only the C-band is used for quantum and classical signals using wavelength division multiplexing (WDM) techniques. In that case, a significant portion of the band will remain underutilized due to the need for spacing between the quantum and classical channels to prevent interference.

Space-division multiplexing has been proposed as a viable approach for classical-quantum coexistence, enabling parallel transmission through multiple spatial channels in a single fiber [8]. A more efficient and affordable approach might involve using multiple bands to allocate separate portions of a wider spectrum to classical and quantum channels, maximizing bandwidth usage and reducing wasted capacity [6]. For instance, the O-band can be used to separate QKD signals from classical ones. This helps minimize crosstalk and leaves the C + L + S-band free for classical channels [9]. Studies and implementations have demonstrated the effectiveness of the O-band for QKD, particularly in optical networks over various distances and applications [10], though dedicating specific bands inevitably reduces flexibility for classical communication and slightly lowers overall spectral efficiency.

However, despite a reduced chromatic dispersion, the O-band introduces additional attenuation in optical fibers, which can impact the secret key rate (SKR), especially in QKD systems deployed over long-distance backbone networks. One practical solution to this issue is implementing trusted nodes (TNs). These nodes act as intermediary relays that extend the range of the QKD system, similar to long-distance QKD implementations over the C-band. TNs effectively divide a long-distance link into shorter segments, each capable of securely transmitting quantum keys, thus mitigating the impact of attenuation and enabling scalable QKD deployment over large optical backbone infrastructures [11].

Due to the higher attenuation of the O-band, QKD networks require more TNs to maintain secure key distribution over long distances. However, this introduces security concerns. TNs must be physically secure and operated in a trusted environment, as they temporarily store and retransmit sensitive key material [11]. If a trusted node is compromised, the security of the QKD system may also be in jeopardy, rendering the exchanged keys vulnerable to attacks. This reliance on the physical and operational security of multiple TNs reduces the theoretical end-to-end security promise of QKD systems [12].

The multipath approach can improve the efficiency and the security of trusted node-based QKD systems [13]. Unlike traditional setups that depend on a single transmission path, multipath QKD distributes quantum keys across multiple network routes. This design enhances resilience against attacks and reduces the risk of key compromise, as an adversary would need to intercept multiple paths simultaneously to retrieve the final key. There are two primary methods for key transmission between QKD transponders (Qponders) in multipath QKD

systems: concatenated multipath (CM) QKD and bitwise product multipath (BPM) QKD. Notably, Qponders encompass all functional entities within a QKD system, including the QKD transmitter (QTx), QKD receiver (QRx), and their respective key distillation engines.

CM QKD methods divide a key into multiple segments, each transmitted through a different path. Once these segments reach the QRx, they are concatenated to reconstruct the original key. This approach enhances security by ensuring that an eavesdropper cannot obtain the complete key without successfully intercepting all the selected paths. Additionally, CM QKD reduces network congestion, as fewer quantum bits are transmitted between Qponders from a single path at any given time. BPM QKD methods transmit multiple independent keys simultaneously over different routes. Once received at the QRx, these keys are combined using bitwise operations to generate a final key. An adversary cannot deduce the final secret key without compromising multiple keys across different channels. However, BPM QKD may introduce additional QKD network congestion due to the increased volume of quantum bits being transmitted [14]. The choice between these two methods depends on the specific security and performance requirements.

2. STATE-OF-THE-ART AND CONTRIBUTION

Multipath QKD networks are increasingly recognized for improving network efficiency and resilience. The authors of [15] propose multipath connections to enhance network workloads by addressing network failures, load balancing, large bandwidth implementation, and low-delay time selection. Similarly, the authors of [16] explore the feasibility of using quantum memories for entangled state distribution, using multipath approaches to mitigate blocking issues. Likewise, the authors of [17] demonstrate that employing multipath routing protocols can exponentially increase the distribution rate of entangled states compared to single-path techniques, highlighting the performance benefits of this method.

Security is a critical consideration in the design of multipath quantum networks. The authors of [18] present a security analysis showing that joint paths offer higher security than non-overlapping or disjoint paths in multipath QKD networks, where disjoint path selection refers to the use of multiple routes between Alice and Bob that do not share any common TNs. The key security enhancement by routing through diverse paths was also discussed in a TN-based QKD network [19]. However, the presence of TNs can create vulnerabilities if they are compromised. To address such risks, the authors of [20] propose separating quantum and public channels across different paths, ensuring that even, if TNs are compromised, the classical information encrypted by the QKD protocol remains secure. Additionally, researchers have explored methods to optimize security and adaptability in multipath quantum networks. The authors of [21] propose separating high- and low-security requests, assigning semi and fully TNs for routing, enhancing network security, and decreasing congestion. While fully TNs offer high reliability and security at a significant cost, semi TNs can perform the

Table 1. Summary of the Related Works

References	Multipath Quantum Networks									
	Blocking Ratio Analysis	Security Analysis	Bitwise versus Concatenated Comparison	C + L + S Nonlinearities on Quantum Signal	Quantum Signal in O-Band	Key Pool Analysis	Propagation Delay Analysis	Single versus Multipath Comparison	Classical and Quantum Traffic Aware	
[13]	X	✓	X	X	X	X	X	✓	X	
[14]	✓	✓	✓	X	X	X	X	X	X	
[16]	✓	X	X	X	X	X	X	✓	X	
[18,19]	X	✓	X	X	X	X	X	X	X	
[23]	X	X	X	X	X	✓	✓	✓	X	
[22]	✓	X	X	X	X	✓	✓	✓	X	
[21]	✓	X	X	X	X	✓	✓	✓	X	
This study	✓	✓	✓	✓	✓	✓	✓	✓	✓	

expected functions more affordably, albeit with increased vulnerability to attacks. The authors of [22] develop a multipath QKD approach that balances quantum key storage while strengthening security requirements.

Recently, the QKD network blocking issue has been addressed in the literature. The authors of [23] introduce a cost-efficient path prioritization method based on the number of TNs and distances, optimizing path selection to reduce the blocking ratio and prevent the waste of quantum keys. Collectively, these efforts demonstrate how multipath approaches improve the performance and security of quantum communication systems, paving the way for scalable and secure quantum networks.

While these prior works lay the groundwork for multipath QKD, a comprehensive analysis that connects blocking, delay, coexistence, traffic awareness, and key synchronization remains missing. This paper aims to fill that gap by introducing a unified framework that addresses these interrelated challenges holistically. Multipath QKD networks improve security against potential attacks and tackle blocking issues; they are affected by propagation delay differences between the paths, a challenge while meeting the required SKR of a QKD system [24]. This paper, as illustrated in Table 1, introduces a comprehensive analysis of multipath QKD systems, addressing critical challenges in security and performance. We propose a novel framework that includes blocking ratio analysis for single and multipath QKD, alongside a comparative security and performance study of BPM versus CM QKD systems. The paper also examines synchronization mechanisms involving key pools at QKD endpoints to efficiently manage keys from multiple paths of varying distances, though this approach raises security concerns. Additionally, we investigate the propagation delay effects in single and multipath scenarios, offering insights into delay minimization strategies.

A significant focus is on the interaction of classical and quantum signals in multiplexed networks, particularly the impact of C + L + S-band nonlinearities on quantum signals and the benefits of using O-band quantum signals to mitigate these effects. We also analyze the balance of quantum and classical traffic loads, identifying the required quantum channel resources to synchronize quantum and classical blocking events. This study provides a holistic view of the trade-offs and enhancements achievable in multipath QKD systems,

advancing the state-of-the-art in secure and efficient quantum communication networks.

The contributions outlined below are structured to reflect key dimensions of multipath QKD system design—performance optimization, delay mitigation, secure key management, and coexistence with classical channels—providing an integrated solution to the open issues discussed above.

- **Quantum-Classical Traffic Awareness:** develops a framework to balance quantum and classical traffic loads, ensuring synchronized blocking events and optimal resource allocation.
- **Blocking Ratio Analysis:** provides a comparative evaluation of blocking rates in a network composed of a C + L + S-band classical network, along with an O-band single-path versus a multipath QKD network.
- **Impact of Classical-Quantum Coexistence:** analyzes C + L + S-band nonlinearities on quantum signals and proposes O-band quantum signal placement to mitigate these effects.
- **Propagation Delay Analysis:** examines the delay effects in single and multipath QKD scenarios and suggests strategies for minimization.
- **Key Pool Synchronization:** introduces mechanisms to manage and synchronize quantum keys across multiple paths while addressing security concerns.
- **Security Enhancements:** investigates the trade-offs between bitwise and concatenated key generation for improved security.

The rest of this paper is structured as follows: Section 3 provides details of the physical layer model assumed for the QKD-classical network. Section 4 introduces our system model, including the proposed classical-quantum resource assignment and routing algorithms with their security and performance analysis. Section 5 introduces the simulation results and discussions on performance and security analysis for classical and quantum communication in the long-distance backbone network. Finally, Section 6 concludes this paper. Moreover, Tables 2 and 3 summarize the notation used throughout the rest of the paper.

Table 2. Table of Notations (Part 1)

Symbol	Description
α_Q	Number of buffered bits per second in the Qponders' pool for a specific lightpath
B_{CQ}	Network blocking rate
β_2	Second-order dispersion coefficient
β_3	Third-order dispersion coefficient
β_4	Fourth-order dispersion coefficient
B_{CR}^r	Classical blocking ratio for each request
B_{QR}^r	Number of blocked paths for each QKD request over the number of paths for the request
C	Compromised secrecy of the final key
CP_s	Compromised secrecy of all paths between the Qponders
d	Destination node
D_p	Propagation delay in microseconds/km
ΔT_p	Path p 's additional time to retrieve its key compared to the time needed for the retrieved key of the shortest path
e_1	Error rate of single photons
e_d	Phase distortion error probability
EGGN	Enhanced Gaussian noise model
E_μ	Quantum bit error rate
η	Probability of receiving at least one photon out of n photons
η_{ec}	Error correction inefficiency
f^i	Channel frequency
f_0	Frequency reference (at wavelength 1550 nm)
$G^{s,i}$	DFA gain
GSNR	Generalized signal-to-noise ratio
γ	Lower bound for SKR in the Decoy-state BB84 protocol
γ_B	Improved SKR with key buffering at Qponders
γ_p	SKR between Qponders
γ_s	SKR in a single-path QKD connection with TNs (minimum SKR between spans)
h	Planck's constant
H	Shannon binary entropy function
ISRS	Inter-channel stimulated Raman scattering
K	Number of different paths
L_p	Distance between Qponders
MBON	Multi-band optical network

3. PHYSICAL LAYER MODELING FOR O-BAND QUANTUM AND C + L + S-BAND CLASSICAL CHANNELS

We assume a multi-band optical network (MBON) with links fully utilizing the C + L + S-band for the classical channels. Following the incoherent Gaussian noise (GN) model for optical transmission links without dispersion compensation [25], the generalized signal-to-noise ratio (GSNR) for a given lightpath on channel i is determined using

$$\text{GSNR}_{LP}^i|_{\text{dB}} = 10 \cdot \log_{10} \left[(\sigma_{\text{ASE}} + \sigma_{\text{NLI}} + \sigma_{\text{TRx}}^{-1})^{-1} \right], \quad (1)$$

where the terms σ_{ASE} and σ_{NLI} are computed as follows:

$$\sigma_{\text{ASE}} = \sum_{s \in S} \frac{P_{\text{ASE}}^{s,i}}{P_{\text{tx}}^{s+1,i}}, \quad (2)$$

$$\sigma_{\text{NLI}} = \sum_{s \in S} \frac{P_{\text{NLI}}^{s,i}}{P_{\text{tx}}^{s+1,i}}. \quad (3)$$

Table 3. Table of Notations (Part 2)

Symbol	Description
MF	Modulation format
M	Number of QRs in the QKD network
μ	Average number of photons per pulse
NLI	Nonlinear interference
p_b	Average number of background noise photons
$p_{\text{dark-current}}$	Background noise from dark current
p_k	Probability that the memories in the Qponders are compromised
p_{NLI}	Background noise from nonlinear interference
p_{SpRS}	Background noise from spontaneous Raman scattering
$P_{s,i}^{\text{ASE}}$	Noise generated by a doped fiber amplifier
$P_{s,i}^{\text{NLI}}$	Nonlinear interference noise power
$P_{s,i}^{\text{rx}}$	Received power at the end of the span s
PS_k	Overall secrecy of path k having N TNs
P_T	Probability that one of the N trusted nodes on the path is compromised by an eavesdropper
$P_{s+1,i}^{\text{rx}}$	Launch power at the start of the span $s + 1$
Q_1	Gain of single photons
Q_k	Length of the keys
Q_k	Length of the final keys in the QKD system
Q_μ	Overall gain
QR	QKD requests
R_{ch}	Channel symbol rate
s	Source node
S	Set of spans
S_k	Secrecy of the divided key for each path in the CM QKD system
σ_{Ag}	Additional SNR margin for aging effects
σ_{Filt}	SNR penalty due to WSS filtering
σ_{TRx}	Transceiver SNR
T_p	Time required to retrieve a key between the Qponders along the path p
T_s	Laser pulse repetition interval
BPM	Bitwise product multipath
CM	Concatenated multipath
QPonders	Quantum transponders
QRx	QKD receiver
QTx	QKD transmitter
TN	Trusted nodes

In these equations, $P_{\text{tx}}^{s+1,i}$ represents the launch power at the start of span $s + 1$, and S denotes the set of spans, while the nonlinear interference (NLI) noise power $P_{\text{NLI}}^{s,i}$ is determined using

$$P_{\text{NLI}}^{s,i} = \frac{16}{27} P_{\text{tx}}^{s+1,i} \times \sum_{\substack{1 \leq n \leq N_c, \\ 0 \leq j \leq 1, \\ 0 \leq k \leq M, \\ 0 \leq q \leq M}} \frac{\rho_n (\gamma^{i,n})^2 (P_{\text{tx}}^{s+1,n})^2 (2 - \delta_{i,n}) (-1)^j e^{-4\alpha_1^n / \sigma^n}}{2\pi (R_{\text{ch}}^n)^2 k! q! (4\alpha_0^n + (k+q)\sigma^n) \beta_2^n} \times \left(\frac{2\alpha_1^n}{\sigma^n} \right)^{k+q} \psi_{i,n,j,k}, \quad (4)$$

where

$$\gamma^{i,n} = \frac{2\pi f^i}{c} \frac{2n_{\text{core}}}{A_{\text{eff}}(f^i) + A_{\text{eff}}(f^n)},$$

and

$$\begin{aligned} \bar{\beta}_2^n &= \beta_2 + \pi\beta_3(f^i + f^n - 2f_0) + \frac{2\pi^2}{3} \\ &\times \beta_4[(f^i - f_0)^2 + (f^i - f_0)(f^n - f_0) + (f^n - f_0)^2], \\ M &= \text{MAX}[10 \times |2\alpha_1^i/\sigma^i|] + 1, \end{aligned} \quad (5)$$

where β_2 , β_3 , and β_4 denote the second-, third-, and fourth-order dispersion coefficients, respectively [26].

Additionally, $P_{\text{ASE}}^{s,i}$, which accounts for noise generated by a doped fiber amplifier (DFA) with a dynamic gain equalizer, is given by

$$P_{\text{ASE}}^{s,i} = n_F \cdot h \cdot f^i \cdot (G^{s,i} - 1) \cdot R_{\text{ch}}, \quad (6)$$

where n_F , h , f^i , $G^{s,i}$, S , and R_{ch} denote the DFA noise figure, Planck's constant, channel frequency, DFA gain, set of spans, and channel symbol rate, respectively. Here, f_0 denotes the frequency reference, which is associated with the wavelength 1550 nm, where β_2 , β_3 , and β_4 are measured. It should be noted that, without loss of generality, we assume the channel bandwidth and the symbol rate are identical. The DFA gain is expressed as in

$$G^{s,i} = P_{\text{rx}}^{s+1,i} / P_{\text{rx}}^{s,i}, \quad (7)$$

where $P_{\text{rx}}^{s,i}$ is the received power at the end of span s . Furthermore, σ_{TRx} , σ_{Flt} , and σ_{Ag} represent the transceiver SNR, the SNR penalty due to wavelength selective switch (WSS) filtering, and the additional SNR margin for aging effects, respectively.

The MBONs considered in this study feature state-of-the-art flexible transceivers capable of dynamically adjusting the modulation format (MF) as long as the GSNR requirements for a given MF are met. This research evaluates the performance of MBONs operating across the C + L + S-band, covering a total bandwidth of 20 THz (6 + 6 + 8 THz). The spectrum is structured into 268 channels, each with a 75 GHz width (6 × 12.5 GHz) and a 400 GHz separation between adjacent bands. The modeling framework employs the enhanced Gaussian noise (EGGN) semi-closed form model to estimate NLI noise, incorporating effects such as Kerr nonlinearity and inter-channel stimulated Raman scattering (ISRS) [26]. This model considers frequency-dependent parameters, including attenuation, dispersion, and nonlinear coefficients. The Raman gain profile is derived by solving coupled differential equations based on pump frequency and offset values.

To further refine the model accuracy, corrections for modulation format and dispersion are incorporated and validated through experimental field trials [27]. Unlike previous works [28–32], this approach assumes a fully loaded spectrum scenario. It integrates a hyper-accelerated flat-received power optimization technique, which includes amplified spontaneous

emission (ASE) noise loading in unoccupied channels, as described in [33].

The O-band of the links is dedicated to the quantum channel, and the lower bound for the SKR (γ) for the assumed Decoy-state BB84 protocol is calculated as in Eqs. (8)–(11) [1]:

$$\gamma \geq \max \left\{ 0, \frac{Q_1 [1 - H(e_1)] - \eta_{ec} Q_\mu H(E_\mu)}{T_s} \right\}, \quad (8)$$

where H is the Shannon binary entropy function, T_s is the laser pulse repetition interval, η_{ec} denotes the error correction inefficiency, and μ is the average number of photons per pulse;

$$Q_\mu = 1 - (1 - p_b)e^{-\mu\eta}; \quad (9)$$

$$Q_1 = \mu e^{-\mu} (p_b + \eta), \quad e_1 = \frac{2\eta e_d + p_b}{2(p_b + \eta)}; \quad (10)$$

$$E_\mu = \frac{\frac{p_b}{2} + e_d (1 - e^{-\mu\eta})}{Q_\mu}, \quad (11)$$

where Q_μ is the overall gain, E_μ is the quantum bit error rate, and Q_1 and e_1 are the gain and error rates of the single photons, respectively. Moreover, e_d is the phase distortion error probability, η is defined as the probability of receiving at least one photon out of n photons, and $p_b = (p_{\text{SPRS}} + p_{\text{NLI}} + p_{\text{dark-current}})$ corresponds to the average number of background noise photons from classical and quantum coexistence, including spontaneous Raman scattering (p_{SPRS}); nonlinear interference (p_{NLI}), i.e., stimulated Raman scattering + Kerr effects; and dark current noise ($p_{\text{dark-current}}$).

4. SYSTEM MODEL AND KEY PERFORMANCE INDICATOR DEFINITIONS

In this study, our system model integrates classical and QKD networks, using the C + L + S-band for classical and the O-band for quantum communication. Classical connections allow grooming and shared paths, while QKD follows a trusted-node model with strict disjoint path selection for security. The proposed resource assignment and routing algorithm selects optimal classical and quantum paths while managing blocking based on channel availability. Moreover, we introduce two new key performance indicators (KPIs) to evaluate the performance of multipath QKD networks in a multi-band optical system. Traditional KPIs are insufficient for assessing this cutting-edge system model, which integrates quantum and classical channels. We begin by examining the most well-known traditional KPI, the SKR, and how the multipath QKD approach influences its calculation. Additionally, buffering techniques are considered to support synchronization within the multipath framework. Since resource availability and security are critical for next-generation QKD-secured optical network operators and their customers, we then define two essential KPIs: (i) the blocking rate, which measures network efficiency in handling QKD requests, and (ii) the security rate, which quantifies the secure key generation capability in the proposed QKD-enabled multi-band multipath optical network.

A. System Model

This section elaborates on the assumptions for the system model, considering both classical and QKD networks operating in the C + L + S-band for classical communication and the O-band for quantum communication. Each service request corresponds to a connection between a QTx and a QRx. With a probability of 10%, a request specifically demands the QKD service to ensure a high level of security for the connection. In the classical network, connection grooming is applied, i.e., multiple requests sharing the same QTx and QRx can be aggregated to optimize resource utilization. However, no grooming is assumed for the quantum network, as the channel establishment follows a trusted-node chain, where quantum links are formed between successive TNs. Furthermore, the routing strategy differs between classical and quantum networks. In the former, the network does not enforce disjoint path selection if there is more than one path between transponders, allowing multiple connections to share links. In contrast, the QKD network employs a disjoint path selection approach, ensuring that quantum connections are established along separate paths to enhance security.

B. Proposed Resource Assignment and Routing Algorithms

This subsection discusses resource assignment algorithms in combined classical and quantum networks. As illustrated in Fig. 1, the process begins by retrieving available channels, frequencies, GSNR, and distances to assess network conditions. First, for classical channels, the shortest paths with the lowest frequencies are identified. The three with the highest GSNR are selected for optimal performance. Next, multiple

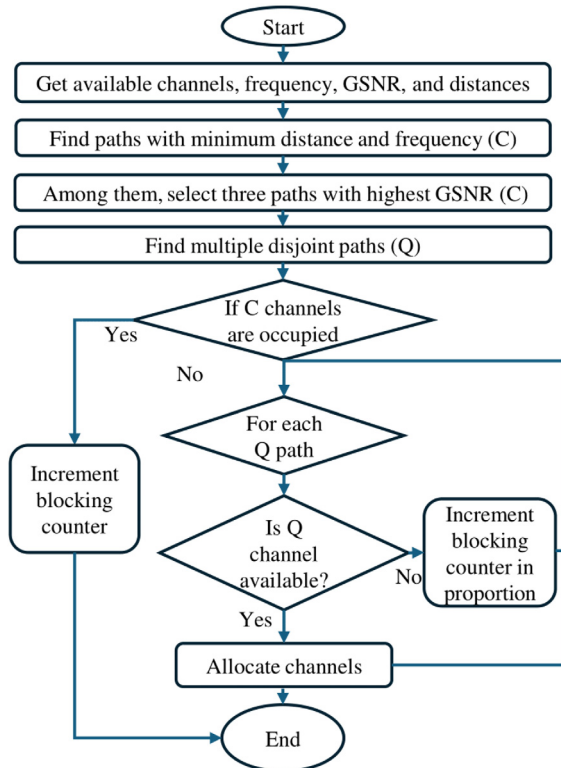


Fig. 1. QKD-classical routing and resource assignment flowchart.

disjoint paths are determined for quantum channels. If all classical channels are occupied, the blocking counter is incremented, and the process ends. Otherwise, each quantum path is checked, and if a quantum channel is unavailable, the blocking counter is proportionally increased. Once all quantum paths are established, the process ends, ensuring efficient and secure QKD-classical channel allocation.

C. SKR and Buffered Keys

The quantum key exchange flow diagram in a long-distance QKD system is shown in Fig. 2(a), where TNs decrypt Alice's quantum key (KA) with the previous TN's quantum key (K_T), then encrypt it with the next TN's quantum key and send it to the next TN/Qponder. Having more TNs due to longer connection distances, which causes propagation delay between edge Qponders, does not affect the overall SKR in the single-path scenario, as they continuously send and receive keys one after another. However, in the multipath QKD scenario, propagation delay across different paths could degrade the SKR due to the QKD network synchronization issue.

Here, γ_p is the SKR between Qponders for the multipath QKD system. It is calculated as in

$$\gamma_p = \min_k \left\{ \frac{Q_k}{T_p}, T_p = (D_p L_p) + \frac{Q_k}{\gamma_s} \right\}, \quad \gamma_s = \min_{\text{spans}} \{\gamma\}, \quad (12)$$

where D_p is the propagation delay in microseconds/km, L_p is the distance between Qponders, T_p is the time required to retrieve a key between the Qponders all through the path p , and Q_k is the length of the keys. γ_s denotes the SKR in a single-path QKD connection with TNs, which is the minimum SKR between its spans. As the propagation delay in multipath QKD decreases the SKR, a solution could be to buffer the shorter paths' keys at the Qponders, allowing continuous key generation in all paths. The improved SKR in this approach (γ_B) would be equal to that of the longest path as defined in

$$\gamma_B = \min_k \{\gamma_s\}. \quad (13)$$

The number of buffered bits per second (α_Q) in the Qponders' pool for a specific lightpath in the QKD network is computed as in

$$\alpha_Q = \sum_{p=2}^K \frac{\gamma_{c_{k=1}}}{\Delta T_p}, \quad k \neq 1, \quad (14)$$

where ΔT_p is the path p 's additional time to retrieve its key compared to the time needed for the retrieved key of the shortest path. The number of buffered keys in all Qponders in the QKD network with respect to connection distance is studied to evaluate the vulnerability of this approach, as the Qponders' key pool can be potentially compromised by an eavesdropper.

D. KPI 1: Blocking Rate

In a multipath QKD network scenario, Fig. 2(b) shows an illustrative example of a six-node MBON and how QKD requests (QRs) from r1 to r7 are served in the network, where

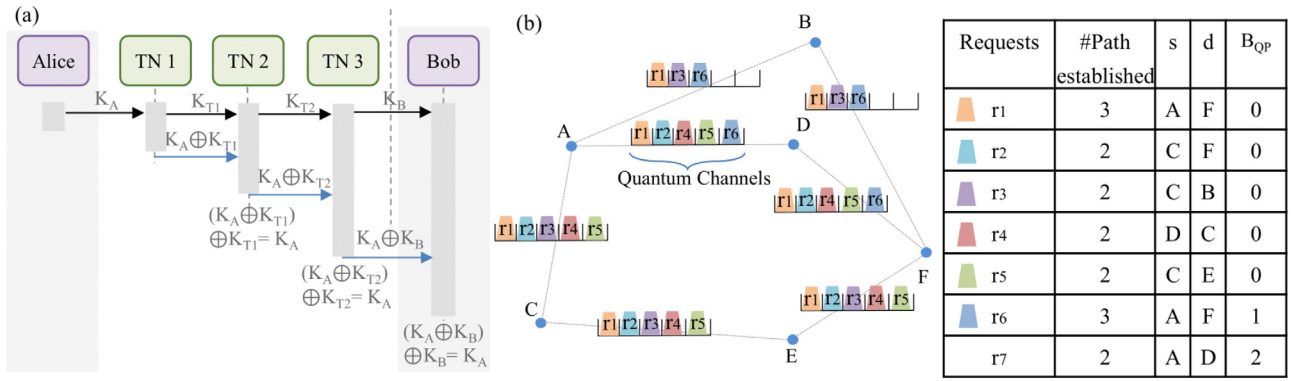


Fig. 2. QKD flow diagram for long-distance QKD with trusted nodes (a) and serving requests in a disjoint multipath QKD system (b).

the requests occupy available quantum channels sequentially based on their arrival order. s , d , and N_{BQR} represent the source, destination, and the number of blocked paths for each QR over the number of paths for the request (B_{QR}^r), respectively. In the example, each request occupies one channel and asks for quantum keys passing through at most $K = 3$ different paths.

Equation (15) shows how the network's blocking rate (B_{CQ}) is computed:

$$B_{CQ} = \frac{\sum_{r=1}^m \max \{ B_{CR}^r, B_{QR}^r \}}{M}, \quad (15)$$

where M is the number of QRs in the QKD network. The classical blocking ratio for each request having QKD security (B_{CR}^r) is 1 if the corresponding classical request is blocked.

To compare different multipath QKD approaches, the BPM QKD system sends the same length keys from different paths between edge Qponders, and once the keys are retrieved from all the paths, a bitwise product is performed on the keys to construct the final key. Although this approach increases security, it increases the blocking rate (B_{CQ}) of the network as well. On the other hand, CM QKD avoids increasing the B_{CQ} while efficiently continuing to use the multipath method, splitting the key into different chunks based on the number of paths and concatenating them once retrieved from all the paths. The former is more secure, while the latter is more efficient, as the injected traffic to the network is similar to that of the single-path approach. As mentioned before, we also assume that the node and link selection in the multipath QKD network is performed so that different nodes and links are selected for different paths, which would enhance the security of the QKD system.

E. KPI 2: Security Rate

We evaluate the security of the QKD system before encountering any blocking issues. This ensures that the analysis reflects the baseline secrecy performance of the network. The overall secrecy of the final key is influenced by the security of individual keys, paths, and the method used to combine keys from these paths. The universal compromised secrecy of the final key between two distant parties is mathematically represented as in

$$C = \prod_{i=1}^n C_i, \quad (16)$$

where C_i denotes the compromised secrecy of each separate key retrieved between the Qponders transmitted over one or more paths, and n represents the number of keys involved in the bitwise product that forms the final key. These formulations are grounded in classical probability theory, where the joint probability of independent simultaneous events is the product of their probabilities. In the BPM QKD system, in which the final key is derived by performing a bitwise XOR operation on keys obtained from multiple paths, the formulation leverages the properties of the XOR operation, where the presence of a single secure key can mask the compromise of others, thereby significantly enhancing the overall security of the QKD system.

On the other hand, in the CM QKD system, where keys from different paths are concatenated to form the final key, the effective secrecy is determined by the probability that all paths remain uncompromised [$n = 1$ in Eq. (16)]. This implies that the overall secrecy decreases as more paths are added, especially if each path has a non-zero probability of being compromised. The compromised secrecy C_i of the concatenated final key is defined as in

$$C_i = 1 - \prod_{k=1}^p S_k(1 - CP_s), \quad (17)$$

where S_k is the secrecy of the divided key passing through the path k , and CP_s is the compromised secrecy of all paths between the Qponders as defined in

$$CP_s = \prod_{k=1}^p (1 - PS_k), \quad (18)$$

where PS_k is the overall secrecy of the path k having N TNs in between, and it is derived as

$$PS = \prod_{T=1}^N (1 - P_T), \quad (19)$$

where P_T is the probability that one of the N trusted nodes on the path is compromised by an eavesdropper. It is important to note that, in BPM QKD, $p = 1$ in both Eqs. (17) and (18),

since a distinct key is obtained from each individual path, and the bitwise product operation is performed across the keys generated from different paths.

The secrecy of the divided key for each path in the CM QKD system (S_k) is computed as defined in

$$S_k = 1 - \frac{\alpha_Q p_k}{Q_k}, \quad (20)$$

where α_Q is the buffered bits collected from the path k , p_k is the probability that the memories in the Qponders are compromised, and Q_k is the length of the final keys in the QKD system.

These formulas are derived from fundamental principles of probability theory and cryptographic security analyses. While specific studies focusing on multipath QKD systems may not directly present these exact formulas, the underlying concepts are well-established. For instance, the security analysis of QKD protocols often involves evaluating the probabilities of different attack scenarios and their impact on the overall secrecy of the key distribution process. Recent research has explored various aspects of QKD security, including using multiple paths and combining keys to enhance robustness against potential eavesdropping. These studies contribute to a deeper understanding of how multipath strategies can be employed to strengthen the security of QKD systems [22,34].

5. SIMULATION SETUP AND RESULTS

In this study, we simulate the U.S. long-haul network, consisting of 14 nodes and 22 links, with distances ranging from 150 to 2400 km, as described in [5]. This network provides a framework to explore the integration of quantum and classical communication systems within a hybrid multi-band architecture. Our analysis primarily focuses on the coexistence of quantum and classical signals and their resulting impacts on network performance and security.

The parameters for the QKD channel simulation in the O-band are carefully chosen based on operational laboratory setups described in [6]. The bandwidth of each quantum channel is set to 12.5 GHz, while the launch power of the quantum channels is set as low as -80 dBm. In contrast, classical channels operate at a significantly higher power of 0 dBm. Additional simulation parameters include a pulse repetition

time in the single-photon detector of 10 ns, an error correction efficiency η_{ec} of 1.16, and a quantum bit error rate e_d of 0.015. The single-photon detectors are assumed to have a quantum efficiency of 0.3, a timing jitter of 100 ps, and a mean photon number μ of 0.5. The receiver's dark-current count rate $p_{\text{dark-current}}$ is extremely low, set at 10^{-8} . The optical fiber nonlinearity coefficient is set to 1.20 1/W/km, and attenuation varies with channel frequency in the range of [0.18–0.38] dB/km, reflecting realistic variations in fiber loss.

The SKR (γ) for all possible 1400 quantum channels defined in the O-band is analyzed under different span lengths of 50, 80, and 100 km. These results are depicted in Fig. 3(a). While the E-band is strategically employed as a guard band to separate the classical and quantum signals, ensuring reduced interference, the SKR gradually declines after 226 THz. This decline is attributed to the increasing nonlinearity effects caused by the interaction of classical signals within the C + L + S-band. Nonlinear interactions, such as four-wave mixing and cross-phase modulation, become more pronounced as quantum channels are placed closer to classical signals, particularly at lower channel frequencies.

After analyzing all possible 1400 quantum channels in the O-band for evaluating the maximum SKR across diverse span lengths, we assume a maximum capacity of 1000 quantum channels operating within the frequency range of 223 to 238 THz for our QKD network, considering a single-path QKD scenario. This upper bound reflects the practical constraint that establishing quantum channels is resource-intensive. These channels demonstrate varying SKRs depending on the span lengths and the relative proximity to classical channels. At these O-band frequencies far from classical channels, the maximum achievable SKR is 800, 100, and 25 kbit/s for span lengths of 50, 80, and 100 km, respectively. It is worth mentioning that, at the highest frequencies, the SKR is significantly decreased to less than 25 and 1 kbit/s for the same span lengths due to the high attenuation rate.

Figure 3(b) illustrates how the span length impacts the SKR when considering a total connection distance of 2500 km. As the span length increases from 70 to 100 km, the SKR experiences a sharp decline, dropping by a factor ranging from 4 to 35, respectively. This confirms that shorter span lengths result in higher SKR due to reduced loss and error accumulation between trusted nodes. However, this improvement comes at the cost of requiring more trusted nodes, which introduces a

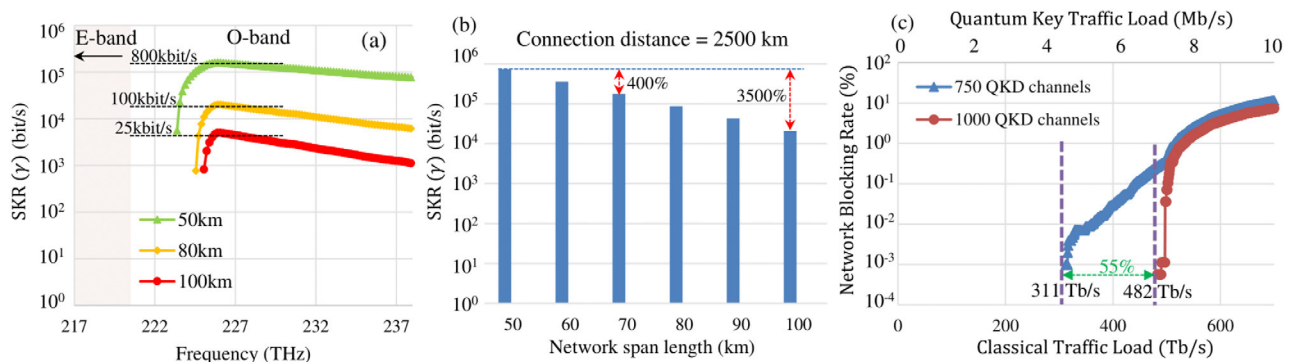


Fig. 3. SKR in O-band quantum link (a), SKR with respect to different network span lengths (b), and bitwise multipath QKD systems without key pool (c).

trade-off: while the SKR increases with shorter spans, more trusted nodes raise system vulnerability—each constitutes a potential likelihood of being compromised—and add significant deployment and maintenance costs. This highlights the need to carefully optimize span intervals to balance both network performance and security.

In this setup, we establish an SKR of 51 kbit/s for each request that requires the security provided by QKD. Furthermore, we estimate that only 10% of the total requests arriving at the classical network will demand quantum keys to ensure their security through quantum encryption mechanisms. The remaining 90% are assumed to function without the need for quantum-level unconditional security, relying instead on standard security protocols. By incorporating these assumptions, we can effectively model the resource allocation and performance of the quantum-enhanced network.

A. Blocking Rate Evaluation

In our QKD network configuration with a 256-bit key length and a propagation delay of 5 μs per kilometer [5], Fig. 3(c) provides a comparative analysis of network blocking ratios under varying quantum channel deployments in the O-band under a single-path QKD scenario. As previously outlined in the system model, network request blocking can occur due to classical or QKD service limitations. In the simulation, the network requests are generated sequentially, with randomly selected source–destination pairs and randomized capacity demands for both classical and QKD traffic. When 750 QKD channels are allocated in the O-band, the first blocking event occurs relatively early, at a classical traffic load of 311 Tb/s and a QKD traffic load of approximately 5 Mb/s. In contrast, increasing the number of QKD channels to 1000 significantly improves performance, reducing the blocking ratio by approximately 55% and delaying the onset of blocking to a classical traffic load of 482 Tb/s and a QKD traffic demand of around 7 Mb/s.

Further detailed examination of the aforementioned network performance is illustrated in Fig. 4. In the scenario with 750 QKD channels, up to 195 Tb/s of classical traffic might be blocked due to insufficient QKD service availability (at least 3 Mb/s of SKR) before classical traffic blocking becomes predominant. Conversely, when 1000 QKD channels are provisioned (serving 7 Mb/s of SKR), classical traffic congestion emerges as the primary blocking mechanism, substantiating the network’s enhanced blocking ratio performance with a 55% reduction in service interruptions.

In the multipath QKD scenario illustrated in Fig. 5(a), without Qponder buffering, the analysis demonstrates a significant degradation of the SKR as longer paths are introduced, which delays key retrieval—since keys from shorter paths must wait for those from the longer ones before the final key can be generated. This synchronization requirement leads to reduced efficiency and contributes to the SKR drop, particularly with increasing connection distances. Specifically, the SKR declines by more than a factor of 3 and 6 when the distance between Alice and Bob extends to 2400 and 7000 km, respectively, contrasting with the stable SKR observed in

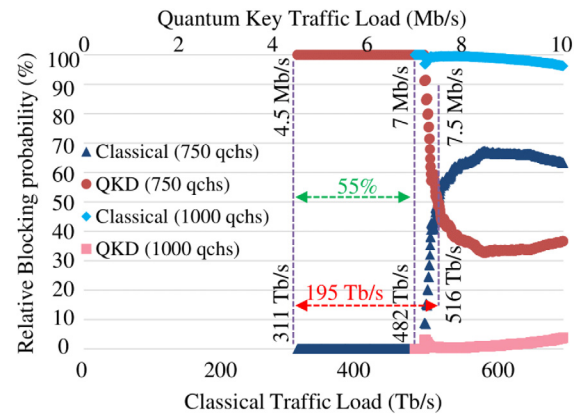


Fig. 4. Classical versus QKD relative blocking probability having 750 and 1000 QKD channels.

single-path configurations where span lengths range between 90 and 100 km.

Figure 5(b) presents the alternative approach utilizing a key pool to mitigate SKR performance limitations. While this method restores multipath QKD performance to levels comparable with the single-path system, for the SKR, it introduces increasing buffered bits of the keys retrieved from shorter paths as connection distances expand. This buffering strategy potentially introduces security vulnerabilities in the QKD system. Comparative results indicate that the BPM QKD system necessitates greater bit storage than the CM QKD system at Qponder sites due to increased QKD traffic transmission. For instance, when the connection distance reaches 7000 km, the BPM QKD system stores three times more bits in the Qponders than the CM QKD.

Figure 5(c) evaluates network blocking rates based on simulated requests for 750 QKD channels, comparing single-path and multipath scenarios across all node combinations. As mentioned before, the network requests are generated one by one with random node pairs and traffic demands for both classical and QKD services. The BPM QKD scenario demonstrates a higher blocking rate compared to the single-path QKD approach, primarily due to increased link occupation under equivalent traffic loads. The CM QKD system exhibits the lowest blocking rate, outperforming even the single-path scenario. This approach enhances network security and improves performance through reduced blocking probability. Consequently, the CM QKD system enables more efficient QKD, serving 7 Mb/s of quantum key traffic load to achieve a blocking ratio comparable to the 1000 QKD channels in the single-path system illustrated in Fig. 3(c).

B. Security Evaluation

The security analysis is performed under the assumption that TNs might be compromised with a 10% probability. At the same time, Qponders’ buffers are significantly less susceptible, with a 1% likelihood of being compromised. The assumed compromise probabilities (10% for TNs and 1% for Qponders) are based on prior modeling studies and threat projections reported in [35], as well as security risk estimates consistent with existing telecommunication infrastructure

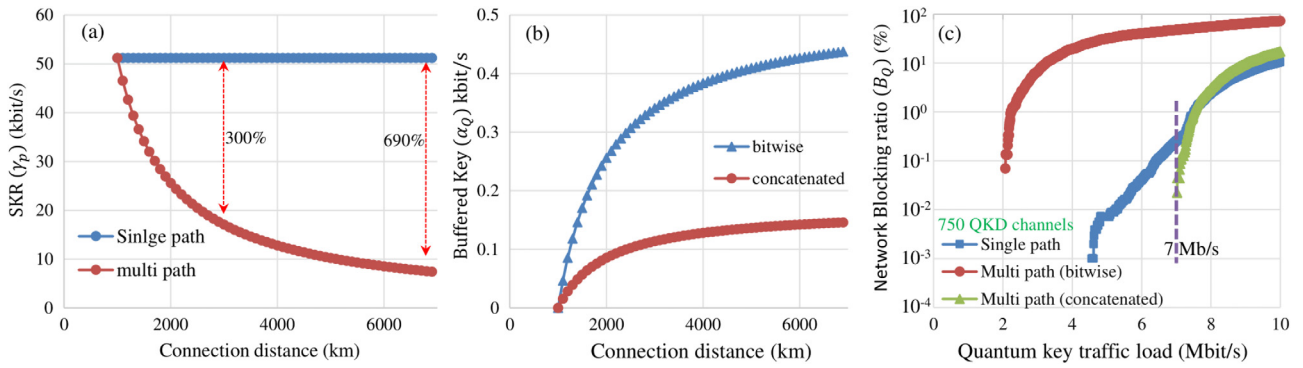


Fig. 5. SKR as a function of connection distance for single-path and multipath QKD scenarios without buffering at Qponders (a). Comparison of buffered key sizes versus connection distance for BPM QKD and CM QKD schemes (b). Network blocking ratio comparison for single-path and multipath (BPM and CM) QKD approaches, assuming 750 QKD channels (c).

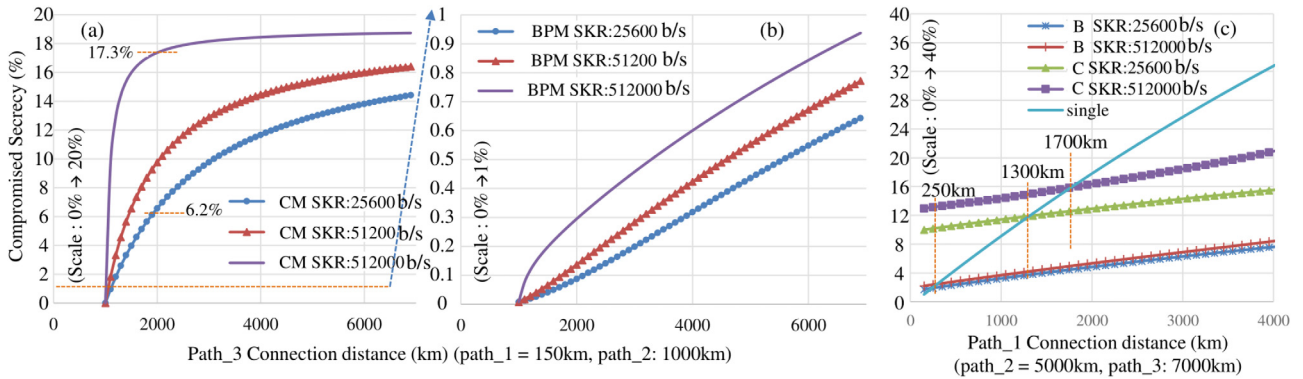


Fig. 6. Compromised secrecy (%) is presented for three cases with varying SKR: (a) concatenated system, (b) bitwise multipath QKD system, and (c) comparative analysis of the single-path, bitwise, and concatenated approaches.

assessments [36]. Buffers at end nodes are less vulnerable because they store keys in secure environments with minimal access. In contrast, TNs are often intermediate repeaters placed across less secure infrastructure. Urban deployments (Qponders) may face increased risks from insider threats, whereas rural infrastructure (TNs) is more exposed to physical tampering or geographic vulnerabilities. This structured approach establishes a quantitative foundation for evaluating potential vulnerabilities within the QKD system, ensuring a clear and measurable framework for assessing security.

Figure 6(a) demonstrates the deterioration of compromised secrecy in the CM QKD system as the connection distance increases. By selecting three SKRs (25.6, 51.2, and 512 kbit/s), the analysis reveals how increased leakage of information from buffered keys at Qponder sites compromises system security. The simulated setup assumes fixed distances for the shortest (150 km) and second shortest (1000 km) paths, with the third path varying from 1000 to 7000 km. This configuration exposes two critical factors affecting compromised secrecy: the number of TNs in the third path and the increasing buffered bits from the first and second paths, consequently increasing the probability of eavesdropper interception. As illustrated, the compromised secrecy is increased by more than 11% when the connection distances of the first, second, and third paths are 150, 1000, and 2000 km, but the SKR increases from 25 to 512 kbit/s. This highlights how increased buffered keys

(leakage information) can compromise the secrecy of the CM QKD system.

However, in Fig. 6(b), the BPM QKD system demonstrates superior security performance compared to the CM QKD scenario. While the CM scenario exhibits up to 20% secrecy compromise, the BPM scenario keeps it below 1% under the same network conditions. This enhanced security is achieved by transmitting different keys through multiple paths, albeit at a significantly higher blocking ratio when utilizing 750 quantum channels. The analysis reaffirms that higher SKRs inherently increase the probability of eavesdropper compromise due to the increased potential for information leakage at Qponders.

Figure 6(c) comprehensively analyzes compromised secrecy in QKD scenarios with fixed second and third paths connection lengths of 5000 and 7000 km, respectively, while systematically varying the shortest path distance between Qponders from 150 to 4000 km. The analysis reveals critical insights into network security performance, demonstrating that multipath approaches offer distinct advantages as shortest path distances increase.

For shortest paths under 250 km, multipath QKD provides no substantive security enhancement and merely increases network blocking rates. However, as the shortest path distances extend beyond 250 km, multipath scenarios progressively outperform single-path configurations. Specifically, for a

512 kbit/s secret key rate, the single-path approach's performance falls between the CM and BPM scenarios. When network capacity permits and high security is essential, the BPM scenario is recommended, particularly for shortest path distances exceeding 1500 km, where both multipath approaches significantly improve QKD network security.

6. CONCLUSION

Using a U.S. long-haul network model, our simulation evaluates the performance of O-band QKD in counteracting C + L + S-band nonlinearities from the perspectives of quantum-classical traffic awareness, blocking ratio, co-existence, propagation delay, key pool synchronization, and security enhancement. The results show a maximum SKR of 800 kbit/s at 50 km span length in single-path configurations, which decreases to 25 kbit/s when spans extend to 100 km. Notably, deploying 1000 O-band quantum channels instead of 750 reduced the network blocking rate by 55%, enabling the network to support classical traffic loads of up to 482 Tb/s.

These findings confirm the critical equilibrium needed when optimizing concurrent transmission of quantum and classical signals in shared infrastructure. Our findings demonstrate that mitigating nonlinear effects is essential for maintaining a robust SKR, particularly when quantum channels operate in proximity to classical wavelengths. Performance of hybrid quantum-classical networks can be considerably enhanced through strategic management of span lengths, guard bands, and channel configurations, establishing a foundation for scalable and secure long-distance communication systems.

Implementing multipath QKD offers dual benefits: enhanced security and delayed network blocking. However, our analysis reveals that, under high traffic conditions, multipath QKD systems experience greater network load compared to single-path implementations. This pattern extends to concatenated disjoint multipath QKD systems, which demonstrate the lowest and most delayed blocking under light traffic conditions but experience the highest blocking rates when the traffic increases. This behavior highlights the trade-offs involved when traffic conditions vary across single and multipath QKD systems.

Our evaluation confirms that multipath QKD's security advantages can be realized without substantial performance drawbacks considering propagation delay analysis and key pool synchronization. The proposed path selection strategies allow for efficiency levels comparable to single-path systems, particularly in low-traffic environments, offering a practical pathway toward next-generation, reliable, and secure long-haul quantum networks. These outcomes align closely with the six contributions outlined in Section 2, offering both theoretical insight and practical design guidance for future quantum-secure backbone networks.

A comprehensive sensitivity analysis on compromise probabilities is identified as an important direction for future research to assess the robustness of multipath QKD networks. Future studies should also address deployment, scalability, and maintenance trade-offs in heterogeneous network environments as QKD systems move toward large-scale implementation. Moreover, physical-layer threats and location-based

vulnerabilities remain important topics for future investigation to enhance the practical resilience of QKD deployments. Finally, ethical considerations, including equitable access and the potential misuse of quantum-secure communications, warrant dedicated examination as QKD technology advances toward widespread societal adoption. It is worth noting that the proposed framework can be extended to advanced protocols, such as measurement device independent (MDI)-QKD and twin field (TF)-QKD [37], with protocol-specific adaptations.

Funding. Wallenberg Center for Quantum Technology, Chalmers University of Technology (101113375-NQCIS); VINNOVA; Vetenskapsrådet; HORIZON EUROPE Reforming and enhancing the European Research and Innovation system (101092766); TUCAN6-CM (TEC-2024/COM-460); Comunidad de Madrid (ORDER 5696/2024).

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, New York, USA, 1984, Vol. 175, p. 8.
2. M. Alshowkan, P. G. Evans, M. Starke, et al., "Authentication of smart grid communications using quantum key distribution," *Sci. Rep.* **12**, 12731 (2022).
3. M. Ahmadian, M. Ruiz, J. Comellas, et al., "Cost-effective ML-powered polarization-encoded quantum key distribution," *J. Lightwave Technol.* **40**, 4119–4128 (2022).
4. H. Hübel, F. Kutschera, C. Pacher, et al., "Deployed QKD networks in Europe," in *Optical Fiber Communication Conference (OFC)* (2023).
5. Y. Mao, B.-X. Wang, C. Zhao, et al., "Integrating quantum key distribution with classical communications in backbone fiber network," *Opt. Express* **26**, 6010–6020 (2018).
6. P. Mehdizadeh, M. R. Dibaj, H. Beyranvand, et al., "Quantum-classical coexistence in multi-band optical networks: a noise analysis of QKD," *IEEE Commun. Lett.* **28**, 488–492 (2024).
7. M. Dibaj, P. Mehdizadeh, M. S. Ghasrizadeh, et al., "From strings to streams: a multi-period analysis of QKD over EONs, showcasing multi-band vs. multi-fiber solutions," in *33rd International Telecommunication Networks and Applications Conference (ITNAC)* (2023).
8. W. Kong, Y. Sun, C. Cai, et al., "Impact of classical modulation signals on quantum key distribution over multicore fiber," *J. Lightwave Technol.* **39**, 4341–4350 (2021).
9. F. Honz, F. Prawits, O. Alia, et al., "First demonstration of $25\lambda \times 10$ Gb/s C + L band classical/DV-QKD co-existence over single bidirectional fiber link," *J. Lightwave Technol.* **41**, 3587–3593 (2023).
10. D. Pan, G.-L. Long, L. Yin, et al., "The evolution of quantum secure direct communication: on the road to the Qinternet," *IEEE Commun. Surv. Tutorials* **26**, 1898–1949 (2024).
11. M. Dibaj, P. Mehdizadeh, H. Beyranvand, et al., "Traffic-aware trusted node placement and resource allocation in multi-band EONs secured with QKD," *J. Lightwave Technol.* **43**, 6–18 (2024).
12. R. B. Walter, O. Krawec, and B. Wang, "Finite key security of simplified trusted node quantum key distribution networks," *arXiv* (2024).
13. M. Wang, J. Li, K. Xue, et al., "A segment-based multipath distribution method in partially-trusted relay quantum networks," *IEEE Commun. Mag.* **61**(12), 184–190 (2023).
14. C. Liu, X. Che, J. Xie, et al., "A multi-path QKD algorithm with multiple segments," *J. Cybersecur. Mobility* **13**, 193–214 (2024).
15. M. Mehic, M. Niemiec, S. Rass, et al., "Quantum key distribution: a networking perspective," *ACM Comput. Surv.* **53**, 96 (2020).
16. H. Leone, N. Miller, D. Singh, et al., "QuNet: cost vector analysis & multi-path entanglement routing in quantum networks," *arXiv* (2021).

17. E. Sutcliffe and A. Beghelli, "Multiuser entanglement distribution in quantum networks using multipath routing," *IEEE Trans. Quantum Eng.* **4**, 4101015 (2023).
18. M. Stepniak and J. Mielczarek, "Analysis of multiple overlapping paths algorithms for secure key exchange in large-scale quantum networks," *J. Inf. Secur. Appl.* **78**, 103581 (2023).
19. M. Wenning, J. Berl, T. Fehenberger, *et al.*, "Improving end-to-end key security in trusted node-based QKD networks with secret sharing," in *Optical Fiber Communication Conference (OFC)* (2025).
20. J. Wang, W. Xue, C. Wang, *et al.*, "Research on multi-path quantum key distribution scheme for hybrid-trusted QKD network system," in *Proceedings of the 2023 5th International Conference on Information Technology and Computer Communications* (ACM, 2023), pp. 6–11.
21. L. Q. Chen, J. Q. Chen, Q. Y. Chen, *et al.*, "A quantum key distribution routing scheme for hybrid-trusted QKD network system," *Quantum Inf. Process.* **22**, 75 (2023).
22. X. Yu, X. Liu, Y. Liu, *et al.*, "Multi-path-based quasi-real-time key provisioning in quantum-key-distribution enabled optical networks (QKD-ON)," *Opt. Express* **29**, 21225–21239 (2021).
23. M. Miao, S. Fang, W. Wu, *et al.*, "Minimum path cost multi-path routing algorithm with no intersecting links in quantum key distribution networks," in *International Conference on Information Systems and Computer Aided Education ICISCAE* (2023), pp. 232–237.
24. J. M. Rivas-Moscoco, A. Melgar, L. Poti, *et al.*, "A reliability plane architecture for ultra-low-energy, high-capacity optical transport networks," in *International Conference on Quantum Communications, Networking, and Computing (QCNC)* (2024).
25. P. Poggiolini, G. Bosco, A. Carena, *et al.*, "The GN-model of fiber non-linear propagation and its applications," *J. Lightwave Technol.* **32**, 694–721 (2014).
26. P. Poggiolini and M. Ranjbar-Zefreh, "Closed form expressions of the nonlinear interference for UWB systems," in *European Conference on Optical Communications (ECOC)* (2022), paper Tu1D.1.
27. Y. Jiang, A. Nespola, S. Straullu, *et al.*, "Experimental test of a closed-form EGN model over C + L bands," *J. Lightwave Technol.* **43**, 439–449 (2024).
28. A. B. Terki, J. Pedro, A. Eira, *et al.*, "Routing and spectrum assignment assisted by reinforcement learning in multi-band optical networks," in *European Conference on Optical Communication (ECOC)* (2022), paper Tu5.63.
29. A. B. Terki, J. Pedro, A. Eira, *et al.*, "Routing and spectrum assignment based on reinforcement learning in multi-band optical networks," in *International Conference on Photonics in Switching and Computing (PSC)* (2023), paper Fr2A.6.
30. N. E. D. E. Sheikh, E. Paz, J. Pinto, *et al.*, "Multi-band provisioning in dynamic elastic optical networks: a comparative study of a heuristic and a deep reinforcement learning approach," in *International Conference on Optical Network Design and Modeling (ONDM)* (2021).
31. M. Gonzalez, F. Condon, P. Morales, *et al.*, "Improving multi-band elastic optical networks performance using behavior induction on deep reinforcement learning," in *IEEE Latin-American Conference on Communications (LATINCOM)* (2022).
32. A. Beghelli, P. Morales, E. Viera, *et al.*, "Approaches to dynamic provisioning in multiband elastic optical networks," in *International Conference on Optical Network Design and Modeling (ONDM)* (2023).
33. F. Arpanaei, M. R. Zefreh, Y. Jiang, *et al.*, "Synergizing hyper-accelerated power optimization and wavelength-dependent QoT-aware cross-layer design in next-generation multi-band EONs," *arXiv* (2024).
34. S. H. Sun, Z. Y. Tian, M. S. Zhao, *et al.*, "Security evaluation of quantum key distribution with weak basis-choice flaws," *Sci. Rep.* **10**, 18145 (2020).
35. S. Rass, M. Mehic, M. Voznak, *et al.*, "Hacking the least trusted node: indirect eavesdropping in quantum networks," *IEEE Access* **12**, 160973–160981 (2024).
36. A. Gaidash, G. Miroshnichenko, and A. Kozubov, "Quantum network security dependent on the connection density between trusted nodes," *J. Opt. Commun. Netw.* **14**, 934–943 (2022).
37. X. Yu, Y. Liu, X. Zou, *et al.*, "Secret-key provisioning with collaborative routing in partially-trusted-relay-based quantum-key-distribution-secured optical networks," *J. Lightwave Technol.* **40**, 3530–3545 (2022).