Optimized Relay-based Quantum Key Distribution for Terrestrial/Non-terrestrial Backhaul Networks

Saurav Kumar Singh[†,1], Sumana Maiti[†,2], Ayan Mondal[‡], and Atri Mukhopadhyay[§]
[†]Department of Computer Science and Engineering, Indian Institute of Technology Bhubaneswar, India
[‡]Department of Computer Science and Engineering, Indian Institute of Technology Indore, India
[§]Department of Electronics and Communication Engineering, Indian Institute of Technology Bhubaneswar, India
{[1]22cs01010, [2]sumana, [§]atrim}@iitbbs.ac.in; [‡]ayanm@iiti.ac.in

***Abstract*—Quantum Key Distribution (QKD) is a critical enabler for secure and future-proof communication in emerging 6G infrastructures, including IoT, vehicular networks, and terrestrial–non-terrestrial (T-NTN) systems. Deployment of QKD over optical X-haul and backhaul networks is cost-effective, as it utilizes existing fiber infrastructure. Combining trusted and untrusted relays lets us stretch communication ranges to build global-scale QKD networks. Hybrid QKD setup uses both trusted and untrusted relays over optical backbone networks, detailing both relay architectures. To reduce the overall cost, we proposed a heuristic algorithm to optimize deployment costs of hybrid network. In this work, we refined that architecture further and explore different ways to improve the proposed algorithm. Moreover, we implemented our proposed scheme and compared the performance with existing schemes, which shows that our scheme requires fewer relay nodes and it reduces the overall cost of the network.**

***Index Terms*—X-haul, Backhaul, security, cost optimization, and quantum key distribution.**

I. Introduction

Quantum key distribution (QKD) is an efficient solution to address cybersecurity issues by exploiting fundamental principles of quantum mechanics [1]. Unlike classical cryptography, QKD ensures security against both present attacks and future cyber attacks by quantum computers. As a result, QKD has emerged as a key enabler for security-critical 6G infrastructures. In emerging 6G-driven IoT, vehicular, and terrestrial–non-terrestrial (T-NTN) networks, the massive data exchange over X-haul and backhaul links demands ultra-reliable and quantum-resilient security mechanisms, for which QKD provides an effective solution.

Due to the quantum nature of QKD signals, amplification is impossible, as dictated by the *No-Cloning Theorem* [2]. Consequently, photon loss cannot be compensated, leading to a limited transmission range. Despite this, substantial progress has been achieved in point-to-point QKD over both optical fibers and free-space channels, making QKD increasingly practical for 6G optical X-haul networks supporting distributed edge computing and IoT services. Recently, successful demonstrations have shown that quantum and classical signals can co-propagate within the same optical fiber [3], [4].

In general, QKD networks rely on trusted relays [5]. These enable long-distance communication by storing local secret keys and forwarding them hop-by-hop to establish global keys [6]. However, trusted relays break end-to-end secrecy, since intermediate nodes access key material and become single points of failure, and the network security is constrained by the weakest relay [6]. This has motivated the use of untrusted relays, where relay nodes never learn the encryption key, thereby preserving end-to-end security [7]. However, untrusted relays incur higher complexity and lower key rates, and two untrusted relays cannot be directly connected; a trusted relay must be inserted to extend the QKD distance [8]. Hence, a hybrid architecture combining trusted and untrusted relays offers a practical tradeoff between security and reach [1].

As a result, a hybrid relay architecture and a heuristic deployment algorithm were proposed in [8] to reduce QKD network deployment cost. In this paper, we further extend this framework for 6G X-haul scenarios by increasing the feasible inter-relay distance and explicitly incorporating physical-layer loss factors relevant to dense optical and T-NTN deployments. The objective is to minimize the number of relay nodes while preserving security and performance, which is essential for cost-efficient, large-scale IoT and edge-computing networks.

To summarize, the contributions of this work are as follows:

1) An improved QKD network architecture that further reduces deployment cost.
2) A modified heuristic cost-optimized QKD backbone networking (MCO-QBN) algorithm that enhances the proposed QKD network's performance and cost-efficiency.

II. General Network Architecture

In this section, we briefly review the QKD network architecture originally presented in [8] [9]. As shown in Fig. 1, the architecture comprises two layers: the QKD layer and the optical layer. The QKD layer deploys a hybrid trusted/untrusted relay-based backbone network consisting of three types of nodes: QKD backbone nodes, trusted relays, and untrusted relays. QKD backbone nodes function as end nodes and supply secret keys to their co-located optical backbone nodes, while trusted and untrusted relays operate as intermediate nodes interconnecting backbone node pairs.

On the other hand, the optical layer in Fig. 1 comprises an optical backbone network in which optical backbone nodes are interconnected by fiber links. To support long-haul transmission, the optical signals are amplified using Erbium-doped fiber amplifiers (EDFAs). Each QKD backbone node is co-located with an optical backbone node. To suppress the

For Personal Use Only

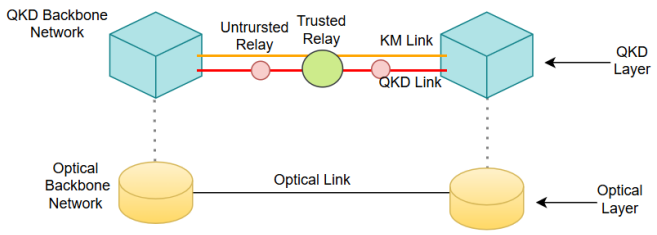


Fig. 1: Hybrid relay-based QKD over optical networks

noise imposed by EDFAs on quantum channels, an EDFA bypass mechanism is adopted using additional MUX/DEMUX elements, such as arrayed waveguide gratings (AWGs). In the existing architecture, relay nodes are co-located with EDFA hubs, thereby restricting the inter-relay distance to the EDFA spacing. Moreover, the overall network security degrades as the number of trusted relays increases.

III. Proposed Architecture

A. Problem Statement

Fig. 1 illustrates the existing hybrid QKD architecture. Let D denote the maximum allowable separation between two consecutive relay nodes, and let l represent the physical distance between two QKD backbone nodes. The required number of relay nodes is then given by

$$N = \left\lceil \frac{l}{D} \right\rceil \tag{1}$$

Since the deployment cost of the network is a function of the number of trusted and untrusted relay nodes, the total cost can be expressed as a monotonic function of N, as detailed in [8]. Consequently, minimizing the network cost is equivalent to minimizing N, which can be achieved by increasing D for a fixed backbone distance l. Accordingly, this work focuses on maximizing D in order to reduce the number of relay nodes required between two backbone nodes.

B. Methodology

In this work, we optimize the number of relay nodes between the backbone nodes to reduce the overall cost of the network. In the existing architecture, the relay nodes are placed at each EDFA hub. This constraint is relaxed in our proposed work, which brings the following challenges.

1) Quantum signals cannot pass directly through EDFA hubs as the amplification process will irreversibly corrupt the fragile quantum states that encode the key information in Quantum Key Distribution (QKD) systems.
2) Allowing quantum signals to travel for longer distances will result in photon losses, which means the distance between two relay nodes should not increase so much to cause significant losses.

Fig. 2 shows that to address the first challenge, our solution keeps MUX/DEMUX at every EDFA hub, which is not a major problem, as the cost of MUX/DEMUX is much less than the cost of the relay node as a whole. Therefore, our architecture can be built as the optical backbone network and MUX/DEMUX at each EDFA hub, similar to the original architecture. The placement of the relay nodes depends on

Algorithm 1 MCO-QBN Algorithm

Input: $G(N, L)$, R, Λ, W_{state}, QBER, MUX, D, η_r, $C_{\max}$
Output: α_{TR}^R, C_{Total}^R, wavelength allocation

intialize $\alpha_{TR}^R \leftarrow 0$, $C_{Total}^R \leftarrow 0$
for each request $r = (s, t) \in R$ **do**
  compute K shortest simple paths between s and t
  $best_cost \leftarrow \infty$, $best_solution \leftarrow \emptyset$
  for each candidate path p_r **do**
    extract edge list $E(p_r)$
    $N_w \leftarrow 3\eta_r + 1$
    $\Lambda_e \leftarrow \{\lambda \in \Lambda : W_{state}[e][\lambda] = 0\}, \ \forall e \in E(p_r)$
    $\Lambda_{common} \leftarrow \bigcap_{e \in E(p_r)} \Lambda_e$
    $S_\lambda \leftarrow \emptyset$, $conv_used \leftarrow 0$
    for $\lambda \in \Lambda_{common}$ **do**
      if $|S_\lambda| = N_w$ **then break**
      end if
      insert λ into S_λ
    end for
    if $|S_\lambda| < N_w$ **then**
      $\Lambda_{pool} \leftarrow \bigcup_{e \in E(p_r)} \Lambda_e$
      for $\lambda \in \Lambda$ in ascending order **do**
        if $|S_\lambda| = N_w$ **then**
          break
        end if
        if $\lambda \in S_\lambda$ **then**
          continue
        end if
        $missing \leftarrow |\{ e \in E(p_r) \mid \lambda \notin \Lambda_e \}|$
        if $conv_used + missing > C_{\max}$ **then**
          continue
        end if
        insert λ into S_λ
        $conv_used \leftarrow conv_used + missing$
      end for
    end if
    if $|S_\lambda| < N_w$ **then**
      continue
    end if
    assign wavelengths per edge using $S_\lambda(e)$
    record C_{Total}^r and α_{TR}^r for p_r
  end for
  Select path with minimum C_{total}^r for r
  $C_{Total}^R \leftarrow C_{Total}^R + C_{Total}^r$
  $\alpha_{TR}^R \leftarrow \alpha_{TR}^R + \alpha_{TR}^r$
  Update network status
end for
return α_{TR}^R, C_{Total}^R, routing and channel allocation for each QKD chain request.

For Personal Use Only

the solution to the second challenge. If we assume that every k^{th} EDFA hub holds the relay node, we should have an upper limit on k to prevent significant loss of information. We can see that our proposed system requires fewer relay nodes.

The required parameters are shown in Table I.

TABLE I: List of Parameters

Symbol	Description
μ	EDFA spacing (km), typically ∼80–100 km
α	Fiber attenuation (dB/km), ∼0.2 dB/km at 1550 nm
L_b	Insertion loss per EDFA bypass (MUX/DEMUX + patching), 1–3 dB
C_r	Cost of one relay (trusted or untrusted)
C_m	Cost of one bypass pair at an EDFA site (MUX/DEMUX + work)
$L_{\max}$	Maximum one-hop loss budget tolerable (28–40 dB depending on system)

Now, D = 2μ in the existing architecture increases to D = $2k\mu$. Hence, N decreases by a factor of k. Therefore, it decreases the cost. The loss per relay to relay hop can be defined as follows.

$$L_{\text{hop}} \approx \alpha \cdot (k\mu) + (k-1)L_b + L_{\text{misc}} \tag{2}$$

where L_{misc} = connectors, filters, co-existence WDM filter margin, etc.

C. Feasibility Constraint

Loss per relay-to-relay hop must be less than the maximum loss tolerable in one hop.

$$L_{\text{hop}} \leq L_{\max} \tag{3}$$

This sets a hard limit on the value of k. Substituting the expressions, we have

$$\begin{aligned} L_{\text{hop}} &\approx \alpha(k\mu) + (k-1)L_b + L_{\text{misc}} \\ &= k(\alpha\mu + L_b) - L_b + L_{\text{misc}}. \end{aligned} \tag{4}$$

Feasibility requires

$$k(\alpha\mu + L_b) - L_b + L_{\text{misc}} \leq L_{\max}, \tag{5}$$

Hence,

$$k_{\max} = \left\lfloor \frac{L_{\max} + L_b - L_{\text{misc}}}{\alpha\mu + L_b} \right\rfloor, \qquad k_{\max} \geq 1. \tag{6}$$

Some practical assumptions are as follows

- $L_{\max} \gg L_b$ (total loss budget much larger than bypass loss),
- L_{misc} is small and can be neglected,
- optionally, $L_b \ll \alpha\mu$ (bypass loss small relative to span loss).

Under the assumption $L_{\max} \gg L_b$, this further simplifies

$$k \lesssim \frac{L_{\max}}{\alpha\mu + L_b}. \tag{7}$$

If the stronger approximation $L_b \ll \alpha\mu$ is applied (so L_b is negligible in the denominator), then

$$k \approx \frac{L_{\max}}{\alpha\mu}. \tag{8}$$

TABLE II: Parameter Setting

Parameter	Typical Range
μ	80–100 km
α	0.19–0.21 dB/km at 1550 nm
L_b	1.5–2.5 dB
C_r	\$5,000–\$50,000
C_m	\$1,000–\$3,000
$L_{\max}$	28–40 dB

This satisfies the problem of photon losses. Moreover, a larger D is achieved, which reduces deployment costs. In the next section, we illustrate the approach using a small example.

IV. Illustration

In this section, we assign some values to the parameters Table I and calculate an approximate value for k. For the time being, we ignore L_{misc}. Parameter values are assigned in Table II.

$$L_{\text{hop}} \approx 0.2 \cdot (k * 90) + (k-1) \cdot 2 \tag{9}$$

Now, using $L_{\text{hop}} \leq L_{\max}$ and $k_{\max}$, we have

$$k \approx \frac{L_{\max} + L_b}{\alpha\mu + L_b} = \left\lfloor \frac{40+2}{0.2 * 80 + 2} \right\rfloor = 2 \tag{10}$$

For example, using these values, we can keep the value of k as 2, which means we can place nodes at every alternate EDFA hub, thereby decreasing the overall cost by a factor of 2. Fig. 2 shows the architecture with $k = 2$.

V. Heuristic Algorithm

Cao *et al.* [8] introduces a cost-optimized QKD backbone networking (CO-QBN) algorithm for fast and cost-optimized solutions in QKD backbone networks. Table III lists all the symbols and definitions used in the algorithm. The key points of the algorithm are summarized below:

- For each request, K shortest paths are computed.
- For each alternating path, the deployment cost and the required wavelengths for quantum signal transmission are calculated.
- The algorithm uses *first-fit* algorithm to choose among various wavelength channels for QKD and KM (Key Management) links.
- The path with the least total cost is selected.
- For each QKD request, the algorithm runs in $O\big(K\big(|N|(|L| + |N|\log|N|) + |W_Q \cup W_M|\big)\big)$ time.

However, the following issues need to be taken care of

- **Wavelength Limitation**: The performance evaluation assumes abundant wavelength availability. In real-world scenarios, not all wavelengths are available simultaneously, which can limit performance.
- **Error Rates**: Quantum Bit Error Rate (QBER) and errors introduced by MUX/DEMUX components are not considered in the original algorithm.

Algorithm 1 presents the complete workflow of the MCO-QBN routing and wavelength-assignment method.

For Personal Use Only

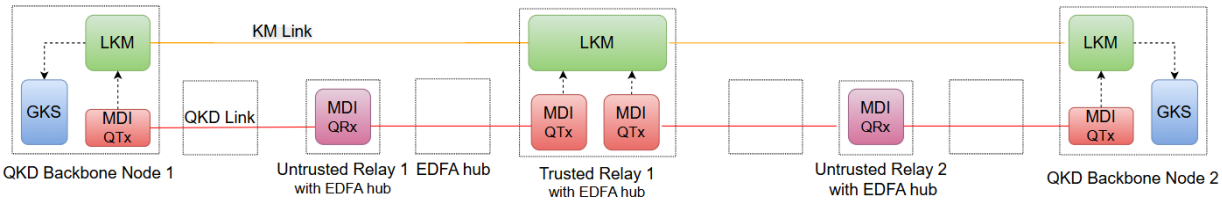


Fig. 2: Proposed QKD architecture with k = 2

Algorithm 2 Calculating cost for each edge on Graph

Input: $G(N, L)$, R, Λ, W_{state}, QBER, MUX, D, η_r, $C_{\max}$, β_{QBER}, β_{MUX}, γ^r_{Tx}, γ^r_{Rx}, γ^r_{KM}, γ^r_{SI}, γ^r_{MD}, γ^r_{Ch}, k
Output: α^R_{TR}, C^R_{Total},

$\alpha_{Tx}, \alpha_{Rx}, \alpha_{KM}, \alpha_{TR}, \alpha_{MD}, l^r_{Ch}, QBER_{max}, MUX_{sum} \leftarrow 0$
for each edge $e = (i, j) \in E(p_r)$ **do**
  obtain physical length $l_{(i,j)}$ of e;
  $\alpha^r_{Tx} \leftarrow \alpha^r_{Tx} + 2\eta_r \cdot \lceil l_{(i,j}/D \rceil$;
  $\alpha^r_{Rx} \leftarrow \alpha^r_{Rx} + \eta_r \cdot \lceil l_{(i,j}/D \rceil$;
  $\alpha^r_{KM} \leftarrow \alpha^r_{KM} + \lceil l_{(i,j}/D + 1 \rceil$;
  $\alpha^r_{TR} \leftarrow \alpha^r_{TR} + \lceil l_{(i,j}/D - 1 \rceil$;
  $\alpha^r_{MD} \leftarrow \alpha^r_{MD} + \lceil l_{(i,j}/D \rceil + \lceil l_{(i,j}/D - 1 \rceil$;
  $l^r_{Ch} \leftarrow l^r_{Ch} + 3\eta_r \cdot l_{(i,j} + l_{(i,j)}$;
  $l^r_{Ch} \leftarrow l^r_{Ch} + (3\eta_r + 1)\, l_{(i,j)}$
  $QBER_{max} \leftarrow \max(QBER_{max},\ QBER[e])$
  $MUX_{sum} \leftarrow MUX_{sum} + MUX[e]$
end for
compute $C^r_{total} \leftarrow \gamma^r_{Tx} \cdot (\alpha^r_{Tx}/k) + \gamma^r_{Rx} \cdot (\alpha^r_{Rx}/k) + \gamma^r_{KM} \cdot (\alpha^r_{KM}/k) + \gamma^r_{SI} \cdot (\alpha^r_{TR}/k) + \gamma^r_{MD} \cdot (\alpha^r_{MD}/k) + \gamma^r_{Ch} \cdot l^r_{Ch} + \beta_{QBER} \cdot QBER_{max} + \beta_{MUX} \cdot MUX_{sum}$;
return α^R_{TR}, C^R_{Total}

For each feasible path, Algorithm 2 computes the total cost by accumulating all deployment-related cost components over its fiber links, adding the conversion penalty, and incorporating two network-quality penalty terms: the maximum QBER observed along the path and the total MUX-induced loss.

The worst case time complexities to process one QKD chain request comprises of $O(K|N|(|L| + |N|log|N|))$ and $O(K(|W_{state}| + |N|))$, respectively. Consequently, the overall time complexity of the MCO-QBN algorithm is $O(K(|N|(|L| + |N|log|N|) + |W_{state}|))$.

VI. Performance Evaluation and Analysis

In this section, we evaluate the performance of the proposed MCO-QBN algorithm and compare it with the baseline CO-QBN scheme. A RANDOM algorithm with random channel allocation is also considered as a benchmark; such random-path routing is commonly adopted in QKD networks [4], [8], [10]. The proposed algorithm incorporates a broader set of loss factors to better reflect practical deployment conditions, which may increase the estimated cost. However, by selectively leaving certain EDFA hubs unutilized, the number of deployed devices is reduced, partially offsetting this increase and improving overall cost efficiency.

Simulations are conducted on two representative network topologies, NSFNET and USNET [8]. QKD chain requests are randomly generated between backbone node pairs, with the K-shortest path parameter set to $K = 3$ to provide three candidate paths per request. In addition, we assume $k = 3$, meaning

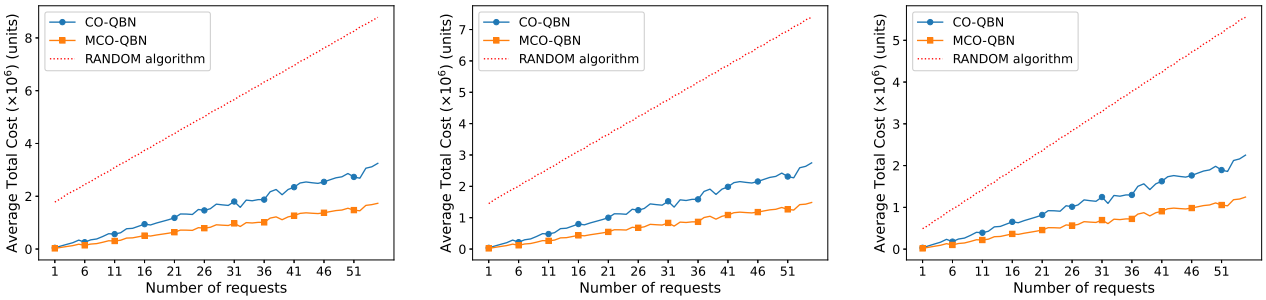
TABLE III: Notations and Definitions

Notation	Definition
$G(N, L)$	Optical/QKD backbone network topology
N	Set of optical/QKD backbone nodes
L	Set of fiber links
i, j	Adjacent optical/QKD backbone nodes in N
$l(i, j)$	Physical length of the fiber link between i and j
Λ	All available wavelengths
W_{state}	Available wavelength channels on each graph edge
D	Distance between a pair of connected MDI-QTxs
$QBER$	Quantum Bit Error Rate for each edge
MUX	Per-hop insertion loss
η_r	Number of parallel QKD links required to satisfy k_r
p_r	Alternative path for QKD chain request r
$L(p_r)$	Set of fiber links on path p_r
R	Set of QKD chain requests
$\mathcal{B}$	{*Tx* = MDI-QTxs, *Rx* = MDI-QRxs, *KM* = LKMs, *SI* = SIs, *TR* = trusted relays, *MD* = MUX/DEMUX pairs, *Ch* = Wavelength Channel, *total* = Total}
α^r_b	Required number of $b \in \mathcal{B}$ for r
l^r_{Ch}	Physical length of QKD and KM link for r
γ^r_b	Cost of an $b \in \mathcal{B}$ for r
C^R_b	Total cost of $b \in \mathcal{B}$ for all QKD requests
K	Number of alternative paths in the K-shortest-path algorithm
$C_{\max}$	Maximum number of wavelength conversions allowed
β_{QBER}	Scaling factor for $QBER$
β_{MUX}	Scaling factor for MUX
k	Number of vacant EDFA hubs between two relay nodes minus one

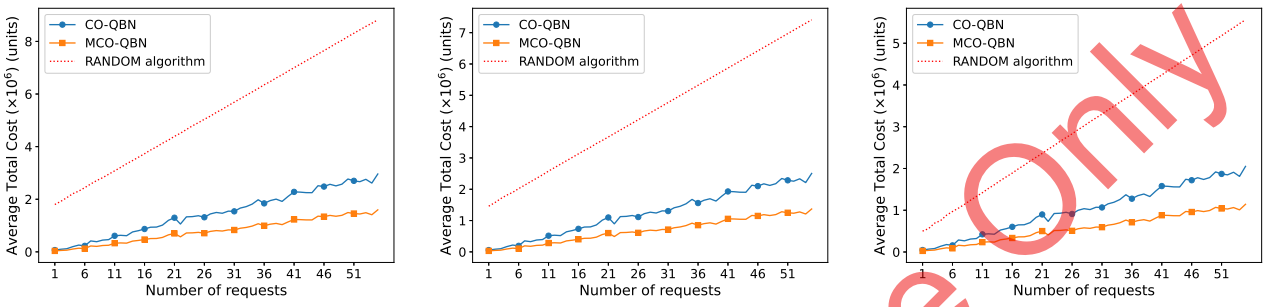
TABLE IV: Cost Values Used for Performance Evaluation

Parameter	SC	UC	DC		
$\lvert\mathcal{R}\rvert$	> 0	> 0	$(0, 0.5\rho]$	$(0.5\rho, \rho]$	$> \rho$
γ^r_{Tx}	1500	[1000,1500]	1500	1250	1000
γ^r_{Rx}	2250	[1500,2250]	2250	1875	1500
γ^r_{KM}	1200	[800,1200]	1200	1000	800
γ^r_{SI}	150	[100,150]	150	125	100
γ^r_{MD}	300	[200,300]	300	250	200
γ^r_{Ch}	[1,2]	[1,2]	[1,2]	[1,2]	[1,2]

For Personal Use Only



(a) Static case based on NSFNET topology (b) Uniform case based on NSFNET topology (c) Dynamic case based on NSFNET topology



(d) Static case based on USNET topology (e) Uniform case based on USNET topology (f) Dynamic case based on USNET topology

Fig. 3: Comparisons of total cost based on NSFNET and USNET topologies

that every third EDFA hub hosts a relay node. Following [8], three cost models are considered: 1) a static case (SC), where device costs do not change with time and is independent of the number of QKD chain requests; 2) a uniform case (UC), where device costs are distributed uniformly within a given range, implying that some QKD chain requests arriving later incur lower deployment cost; 3) a dynamic case (DC), where device costs depend on the number of QKD chain requests, i.e., the cost decreases as the number of requests increases. The normalized device cost values are listed in Table III. Since practical cost figures are not publicly available, these values are assumed relative to link cost based on representative systems [8]. The simulation results are shown in Fig. 3. It can be observed that the total deployment cost is significantly reduced across all cases, primarily due to the improvements introduced in the proposed architecture.

VII. Conclusion

In this paper, we proposed a cost-efficient QKD relay-based architecture for optical backhaul networks. We showed that the total deployment cost can be reduced by a factor equal to the number of EDFA hubs between two relay nodes, while simultaneously improving security by reducing the number of trusted relays. The CO-QBN algorithm was further enhanced by incorporating wavelength availability and error-rate constraints along with the architectural improvements. The original and modified algorithms were evaluated over two network topologies under varying request sizes. The results confirm the suitability of the proposed approach for secure and scalable QKD deployment in both terrestrial and non-terrestrial network environments supporting future 6G X-haul infrastructures.

References

[1] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.

[2] W. K. Wootters and W. H. Zurek, "A single quantum cannot be clonedk," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[3] A. Aguado *et al.*, "The engineering of software-defined quantum key distribution networks," *IEEE Communications Magazine*, vol. 57, no. 7, pp. 20–26, Jul. 2019.

[4] C. Le Quoc, P. Bellot, and A. Demaille, "Stochastic routing in large grid shaped quantum networks," in *Proceedings of the IEEE International Conference on Research, Innovation and Vision for the Future*, Hanoi, Vietnam, Mar. 2007, pp. 166–174.

[5] X. Ma, R. Annabestani, C.-H. F. Fung, H.-K. Lo, N. Lütkenhaus, D. Pitkänen, and M. Razavi, "Quantum network with trusted and untrusted relays," p. S1.330, 2012.

[6] Y.-A. C. C.-Z. P. Q. Zhang, F. Xu and J.-W. Pan, "Large scale quantum key distribution: Challenges and solutions [invited]," *Opt. Exp.*, vol. 26, no. 18, pp. 20–26, Sep. 2018.

[7] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Physical Review X*, vol. 6, no. 1, p. 011024, 2016.

[8] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 9, pp. 2834–2849, Sep. 2021.

[9] J. He, Y. Zhou, S. Xie, and C. Wang, "A cost-optimal quantum key distribution based on hybrid trusted relays," in *Proceedings of the 2025 International Conference on Big Data, Communication Technology and Computer Applications (BDCTA 2025)*. Kuala Lumpur, Malaysia: ACM, Feb. 2025, pp. 1–9.

[10] H. Wen, Z. Han, Y. Zhao, G. Guo, and P. Hong, "Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network," *Science China Series F: Information Sciences*, vol. 52, no. 1, pp. 18–22, Jan. 2009.

For Personal Use Only