A Topology-aware Quantum Inspired Genetic Algorithm for Secure Quantum Communication

Saumya Priyadarshini, Chandrashekar Jatoth, *Member, IEEE*, Rajesh Doriya, *Senior Member, IEEE*, Rajkumar Buyya, *Fellow, IEEE*

***Abstract*—Quantum communication ensures that data remains secure from unauthorized access. Despite these advantages, this technology faces several challenges. For instance, photons can be lost when they go through channels, and there is a chance of eavesdropping, that make the system not as trustworthy, safe, and efficient. To make quantum communication systems function effectively in the real world, we need to combine advanced technologies like quantum error correction mechanisms and quantum repeaters. This work suggests a unified Quantum Inspired Genetic Algorithm (QIGA) framework that utilizes collaborative quantum repeaters to conquer the limitations of network links over distance. This study introduces a hybrid optimization topology (OT) that integrates mesh, star, and ring configurations for measurement device-independent quantum key distribution (MDI-QKD) networks. This approach allows for the efficient use of resources for scalable quantum communication networks. The proposed network architecture integrates 12 user nodes, a trusted node, and a single shared quantum repeater within a hybrid topology. The repeater deployment has been designed to support links that are longer than 52 km. This design accommodates deployments on various scales, small, medium, and large, while optimizing resource usage and infrastructure costs. We evaluated the performance and security trade offs in quantum communication networks by optimizing three topologies with a QIGA: ring, ring-star, and ring-star-mesh hybrid ($QIGA-OT$). The optimization methodology aims to reconcile essential performance metrics, such as the Secure Key Rate (SKR), Quantum Bit Error Rate (QBER), channel loss, and Merit of Quantum Efficiency (MQE). MQE functions as a metric for evaluating trades concerning security, efficiency, and cost-effectiveness within the network. This work presents a novel approach for utilizing quantum-inspired in the effective design and implementation of scalable network topologies across numerous fields of application.**

***Index Terms*—Network topologies, Quantum teleportation, Quantum entanglement, Quantum protocols, Security, Quantum Inspired Genetic Algorithm (QIGA), Measurement device independent (MDI-QKD).**

I. Introduction

RECENT advancements in quantum computing have generated significant interest in technology capable of constructing networks of quantum computers [1]. Quantum communication is a method that makes it possible for different quantum computers and devices to connect with each other, for building a quantum network [2]. The main objective of quantum communication is to transfer photonic entanglement over extended distances between the nodes that are involved [3]. This technique establishes a quantum channel that preserves the inherent quantum correlations of entangled particles [4]. This channel serves as an essential resource for advanced communication protocols, which have no classical equivalents. These include quantum teleportation, which transmits an unknown quantum state without physically transmitting the particle, and QKD which creates and securely exchanges keys based on quantum principles [5]. The ability to extend entanglement over huge networks is important for making quantum communication systems secure and flexible [6].

Quantum communication facilitates enhanced information security unattainable through tradational communication [7], [9]. The concepts of qubits, entanglement, teleportation, and superposition have made this security achievable. The no-cloning theorem hinders individuals from intercepting qubits, and quantum teleportation ensures that communication is secure [8], [10]. This guarantees data can be shared securely while also making it possible to find anyone who is eavesdropping on the network. Researchers have shown that certain features of quantum communication make it more secure than classical communication [11]. These achievements have been accomplished via free-space and fiber optic cables, demonstrating that remote quantum communication is progressively feasible [12]. Quantum communication networks encounter significant obstacles in facilitating multi-user scenarios due to inbuilt physical limitations, including decoherence, photon loss, and the no-cloning theorem [13], [14]. The technological limitations associated with quantum repeaters, error correction, and hardware that requires a lot of resources. Quantum repeaters, quantum memory, generalized quantum measurements, qudit, hyper-entanglement, trusted nodes, active switching, and other technologies have helped to reach this goal [15]. These improvements make quantum networks work more effective and develop wider. QKD employs the principles of quantum physics to securely transmit encryption keys [16]. In large networks with numerous users across vast distances, it is challenging to establish direct connections between each pair of users [17]. The development of a global quantum network may enable breakthrough technologies that are currently unavailable [18]. It would make it possible for quantum computers to be connected globally and qubits to be transmitted instantly. In addition, such a network could greatly improve communication security. To rectify this, QKD must be integrated into a broader network to facilitate increased user connectivity and extend the communication range [19].

A qubit is the quantum equivalent of a classical bit that can exist in a superposition of the two quantum states, $|0\rangle$ and $|1\rangle$ [20]. A quantum network comprises interconnected quantum devices, such as quantum computers, sensors, repeaters, that

Manuscript received April 15, 2026;

transmit quantum information via quantum communication methods [21]. It includes nodes, networks, quantum repeaters, decoherence through entanglement, and classical channels [23]. Quantum networks can be classified as local restricted to a single place, metropolitan extending across cities for purposes like QKD or teleportation, and global constituting the foundation of the quantum internet [24], [25].

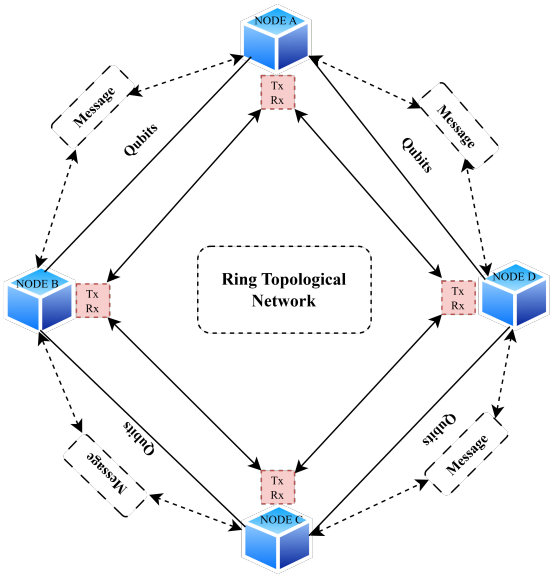

Fig. 1. Ring topology network architecture conceptual diagram: The diagram presents nodes organized in a circular configuration, establishing a continuous closed circuit through which data packets are transmitted sequentially.

The primary attributes encompass QKD protocols, including BB84 [4], and E91 [4], which enable the secure key exchande by identifying eavesdropper. Quantum topology investigates the formation and interrelationship of quantum networks [26], [27]. Examines the connections of quantum devices, such as computers or nodes, utilizing quantum channels, such as optical fibers or free-space networks [30]. There are several approaches to generate these networks. One configuration is point-to-point [22], [28], as shown in Fig. 1 as an example of qubit based message transmission. A ring topology network model consists of four nodes Nodes A, B, C, and D have been developed within the framework of quantum communication. A loop that links each node to its adjacent ensures uniform and consistent communication channels in this design. Each node contains a Tx and Rx as transfer and receiver for secure message transfer via qubits. This method allows efficient qubit transfer between any two nodes and provides a scalable framework with network security, latency, and reliability. Another configuration is star topology, wherein a central node such as a quantum repeater interconnects multiple peripheral nodes, rendering it advantageous for metropolitan implementations. Mesh topology [9], connects nodes in numerous ways, offering data in multiple ways to get from one place to another. This makes the network more flexible and makes it easier to grow.

Hybrid topology combines quantum and classical links to integrate with existing internet infrastructure and shared entangled states to support advanced functions like teleportation and distributed quantum computing [17], [29]. The quantum topology provides the physical and logical foundation for networks that regulates the implementation of quantum communication. It affects the competence of quantum protocols by influencing latency, entanglement quality, SKR and scalability by establishing the basis of the quantum Internet [15]. Thus playing a crucial role in the development of reliable and efficient quantum communication systems.

The main contributions of the paper are summarized as follows:

1) To improve network scalability and reliability, a novel fault tolerant hybrid framework $QIGA-OT$, for quantum communication networks, has been proposed that combines mesh, ring, and star topologies.
2) The integration of decoy state and MDI-QKD protocols enables a comprehensive evaluation of channel noise, eavesdropping threats, security, and connection efficiency.
3) An approach is employed to position a share repeater at the center of extended link endpoints by minimizing the signal loss and enhancing the SKR for long distance quantum communication links.
4) A QIGA has been introduced using decoy state approaches that optimize the path in the hybrid topology and enhance the MQE.

The rest of the paper is structured as follows: Section II, presents an overview of the related research work. Section III, presents the methodology of the quantum communication network model. Section IV, provides a performance evaluation, followed by an analysis of the results, conclusions and future work in Section V.

II. Related Work

Due to significance in quantum communication, including protocols, communication approaches, various mechanism like entanglement based, QKD, Quantum Secret Channel (QSC), Direct quantum communication, quantum repeater and long distance, it is categorized into traditional approaches and quantum based optimization approaches.

A. Classical Quantum Approaches

To contribute the advance study of quantum networks, several pioneering investigations have been conducted over the years. To provide a few instances, Chandra et al. [31] proposed a technique for constructing Quantum Topological Error Correction Codes by mapping classical topological codes into the quantum theory via a classical to quantum isomorphism. They developed classical codes utilising lattice structures and transformed them into quantum stabiliser codes that facilitate fault-tolerant quantum processing. In [32], the author addressed the challenge of ensuring secure quantum communication, to address the shortcomings of previous methods that necessitated on comprehensive knowledge of the network architecture. They proposed a quantum network coding scheme that guarantees both data confidentiality and accuracy without requiring classical communication. Their approach enhances traditional secure network coding techniques by utilising invertible matrix operations at each node. A scalable, fully linked quantum

communication network connecting eight users without dependence on trusted nodes [33], [40], effectively established 28 secure quantum key distribution links via a single entangled photon source. The passive multiplexing via wavelength filters and beam splitters, requiring minimum hardware only one fibre and two detectors per user providing superior scalability and practical application compared to previous methods.

In the presence of powerful quantum adversaries, Bullock et al. [34] investigated covert communication across lossy thermally generated bosonic channels. They established the highest possible covert rate of transmission and showed that modulation using QPSK with coherent states performs better than BPSK. This research provides a robust and pragmatic basis for undetected quantum communication, surpassing previous classical techniques [35], [37]. The author present a $4,600$ km quantum communication network, integrating a $2,000$ km fibre network with more than 700 QKD, links and two satellite-to-ground QKD links, achieving a key rate of 47.8 kbps, 40 higher than previous outcomes. It makes use of distant and twin-field QKD innovations and is based on fundamental QKD frameworks. Chen et al. [36] analyzed the quantum communication capacity of complex quantum networks using an information-theoretic framework, with particular emphasis on the influence of node density and underlying network architecture. In parallel Li et al. [43] proposed an enhanced framework for establishing remote entanglement in quantum lattice networks, where each inter-node connection is subject to capacity limitations.

Quantum decoherence limits require QoS [22], for delay and entangled distribution rates. They detect constraints in quantum network protocols, specifically their inability to support different network topologies [42]. Granelli et al. [46] integrate quantum and traditional communication networks for QKD and distributed quantum computing. The author in [25], discussed about how to keep end-to-end entanglement fidelity in quantum networks, which is necessary for things like QKD. The protocols that are currently in effect often are unsuccessful because interference is included during entanglement swapping. They proposed a greedy algorithm to resolve this issue and enhance resource allocation among numerous source destination pairs. Analysis of the simulations demonstrated that throughput, fidelity, and overall resource utilization were all superior than those were with conventional approaches. Illiano et al. [48] examined the challenges encountered when attempting to implement classical Internet protocols on quantum networks [44]. They said that basic quantum principles, such as the no-cloning theorem, superposition, and entanglement [45], render traditional methods, such as data replication, useless. To solve the problem [23], the author advised altering the quantum protocol stack to enable entanglement-based secure communication and quantum teleportation. This restructuring should make quantum networks work more effectively by allowing new connections and making it easier to allocate and route resources. These improvements are necessary for the quantum internet to work [39].

Wang et al. [49] further contributed by demonstrating that the twin-field (TF-QKD) protocol enhances the efficiency and range of QKD. They were able to send secure quantum keys over an 833.8 km optical fiber, setting a new record for network loss tolerance of more than 140 dB. This work directly addresses the exponential reduction of key rates caused by network loss over long distances, thereby pushing the fundamental limits of scalable QKD implementations. The study addresses receiver-end concerns that slow application performance such as video conversations and reduced SKR [50], detector efficiency, and data processing. They use a single-decoy state to simplify the BB84 protocol, improve sifting, and secure key transfer over ultra-low-loss optical fibers. Shen et al. [51] introduce a quantum teleportation system that addresses the challenges of achieving high-fidelity, high-rate quantum teleportation over metropolitan distances. They suggest a solution utilising a high-efficiency time-bin entangled photon source. Chawla et al. [52] discussed two directly connected quantum network nodes can communicate securely using a quantum walk protocol. The necessity for secure, high-fidelity quantum communication [38], channels for effective long-distance communication and quantum computing is discussed in the paper. Zhang et al. [53] investigate how fiber-friendly LNOI micro-waveguides might enhance nonlinear photonics for regular and quantum applications. Due to poor signal connection and complex manufacture, thin-film lithium niobate (TFLN) makes it difficult to build excellent, scalable devices. Shi et al. [54] describe a star shaped continuous variable quantum teleportation infrastructure with one central station and numerous user nodes. They generate and convey many entangled signals of light from a compressed light source using optical controllers and the frequency combs.

B. Quantum Inspired Optimization Approaches

Anwar et al. [55] investigate the mechanics of entanglement within the quantum network system. They concentrate on the issue of an entanglement diminishing during transmission due to noise and interference, which impacts the efficacy of flexible quantum systems. The progress in the field of quantum photonics [56], by showing experimentally that time-bin and energy-time entanglement can be achieved without the post-selection loophole, using a chip-based device. Their main point is that using classical methods on standard setups for creating this type of entanglement can trick them into giving false quantum results, which makes quantum communications [41], [58], less secure. Yang et al. [57] discussed that entangled photons are transferred between users, and the noise keeps their quality high even after vast distances. Their investigations demonstrated that entangled photons retained over 85% quality after 300 km, enabling secure direct communication between all users. Saad et al. [59], proposed a quantum-inspired genetic algorithm (QIGA) for the Resource-Constrained Project Scheduling Problem by integrating quantum concepts (Qubits, superposition, and quantum gates) to improve exploration and avoid premature convergence. The algorithm employs quantum initialization, specialized crossover and mutation, and a serial schedule generator to maintain feasibility. It demonstrated competitive performance against others. The study suggests future work on incorporating quantum interference and further hybridizations for enhanced scalability. Xu et al. [60], propose

a novel hybrid optimization framework for designing planar multilayer photonic structures. This strategy innovatively combines a QIGA with a machine learning surrogate model specifically a Random Forest (RF) regression model within an active learning scheme. The QIGA enhances the performance of classical GA by integrating quantum mechanical principles, resulting in faster convergence and greater algorithmic robustness. The study [61], introduces a comprehensive hybrid metaheuristic suite. In order to advance the discipline, it integrates GAs with quantum-inspired computing to expand search capabilities. It utilizes reinforcement learning to adjust parameters throughout the process and implements error-correcting codes to manage system faults. Adopts dynamic resource allocation to improve energy efficiency, and incorporates deep reinforcement learning to strategically direct the search process. Novel hybrids with QIGA are evaluated using a Quantum-inspired Benchmarking Framework. Thus, laying the groundwork for next-generation dependable and efficient quantum communication systems.The primary research [62], examines QIGAs, which constitute an innovative methodology in evolutionary computing. The research suggests utilizing quantum physics concepts, such as superposition and interference, to improve the efficiency of GAs. This study is primarily theoretical, emphasizing core principles and contrasting quantum-based genetic algorithms with classical ones. The research conducted by Dung et al. [63], represents an important step forward in QIGAs. These algorithms use qubits to encode data and take advantage of superposition and probabilistic convergence. This lets them search complex solution spaces more thoroughly and effectively than standard GAs. The study introduces a floating-point encoded QIGA for the dynamic transportation network design problem, expanding this new area. The method exceeds classic GAs on well-known reference networks while requiring fewer computing resources, such as smaller population sizes. Quantum-inspired methods can solve complex infrastructure planning optimization problems, according to the research.

Therefore, prior research efforts aimed at designing optimal communication networks for secure data transmission particularly those emphasizing end-to-end entanglement distribution through resource allocation and quantum operations often reveal constraints in scaling to large-scale quantum networks and in providing reliable, guaranteed service levels.

III. Methodological Framework

This work suggests an optimization framework based on a QIGA to solve the problems of getting secure and scalable QKD across metropolitan-area networks. The method finds good hybrid network topologies that mix ring, star, and mesh structures and are specifically made for MDI-QKD. The framework enables dependable, long-distance secure key generation by integrating quantum repeaters on links that surpass the maximum transmission range and employing a trusted node for Bell-state measurements.

In this section, we propose a $QIGA - OT$ framework in Fig. 2 to establish a reliable and efficient quantum communication network that ensures optimal performance and stability. Creation of physical models of MDI-QKD links, network setup with trusted nodes and repeaters, evolutionary optimization, and network testing under normal and eavesdropping conditions are the steps. Repeaters for networks beyond a transmission threshold regulated by a central trusted node simplify long-distance secure key distribution.

The proposed framework is structured into six sequential stages, are mentioned as: Hybrid Quantum Network Modeling and Node Deployment, Physical-Layer MDI-QKD Channel and Device Modeling, Decoy-State Parameter Estimation via Linear Programming, SKR Computation and Security Evaluation, Hybrid Topology Optimization using QIGA, Multi-Criteria Performance Evaluation and Result Analysis. First, a hybrid quantum network model is created by deploying user nodes, a trusted node, and repeater nodes in a two-dimensional area. The distances between the nodes are calculated, subject to constraints on the maximum link length. Second, a thorough physical-layer MDI-QKD model is designed to accurately represent quantum communication links, accounting for optical channel transmittance, photon statistics, detector efficiency, dark counts, and misalignment errors. Third, decoy-state parameter analysis is performed using linear programming to securely bound the single-photon yield $Q1$ and error rate $e1$, thereby ensuring unconditional security guarantees for MDI-QKD. Fourth, the SKR as R and QBER are calculated using these parameters under both normal and eavesdropping condition, facilitating rigorous security assessment. Fifth, QIGA optimizes the hybrid network topology by encoding ring, star, and mesh configurations, adaptively evolving populations of candidate solutions, and repairing infeasible long-distance links via trusted nodes and repeaters. Finally, the optimized topology is evaluated using a multi-criteria performance metric MQE, framework that jointly optimizes SKR, QBER, transmission loss, and infrastructure cost. Convergence analysis and visualization demonstrate the approach's effectiveness and robustness.

As a result, communication loss is reduced, network scalability is increased, and eavesdropping resistance increases. The suggested framework uses robust error correction mechanisms and dynamic topology adaptation to achieve high efficiency while ensuring secure key generation. $QIGA-OT$ framework comprises user nodes, a central trusted node, and a shared quantum repeater to support long-distance connections exceeding 52 km. Quantum repeaters minimize photon loss and decoherence in distant connections by entanglement swapping and purification. Error-correction strategies facilitate low QBER, support multi-hop QKD, and sustain a viable SKR [1], [15]. A firewall is installed at the conventional interface to secure the control and key management channels against unauthorized access, denial-of-service attacks, and side-channel vulnerabilities that may affect the integrity of the quantum link [28]. Additionally, a unified switching system enables dynamic routing [47] and efficient interoperability across quantum and traditional channels, enhancing data transmission across various topologies. This incorporates cyclic pathways in ring networks, the centralized hub of star networks, and the interconnected structure of mesh networks, consequently diminishing latency and enhancing throughput. The data center in the network core accommodates QKD servers and traditional storage systems

to oversee entangled states, authenticate users, and facilitate centralized data aggregation across all linked nodes.

Let the set of nodes be defined as $User1$, $User2$, …, $UserN$, representing the endpoints requiring secure quantum communication; a trusted node T serving as a $MDI-QKD$ center; and the repeater node set $R = \{R_1, R_2, \ldots, R_k\}$, which facilitates long-distance quantum communication through entanglement swapping. The trusted node facilitates QKD operations, enables multi-hop relaying, and supports network management. The physical distance between any two nodes i and j is determined by the Euclidean metric. A physical constraint is imposed through the maximum permissible fiber distance $d_{\max}$, which represents the practical limit for direct MDI-QKD implementation. This constraint emerges from the exponential attenuation of quantum signals in optical fibers, where transmittance follows Equation (1), with α being the attenuation coefficient and d the transmission distance. When the direct distance between two user nodes exceeds $d_{\max}$, the resulting signal loss renders secure key generation infeasible.

To address this limitation, a link repair mechanism is implemented. For any user pair (U_i, U_j), where the distance $d_{ij} > d_{\max}$, the direct link is replaced by a two-hop path through an intermediate node $I \in \{T\} \cup R$. The intermediate node selection must satisfy the distance feasibility conditions.

$$\eta(d) = 10^{-\alpha d/10} \tag{1}$$

$$I^* = \arg \min_{I \in \mathcal{I}_{\text{feasible}}} (d_{i,I} + d_{I,j}) \tag{2}$$

Equation (2). selects the optimal intermediate node I^* from the set of feasible nodes such that the total path length from node i to node j via I is minimized. Specifically, it identifies the trusted node that yields the shortest two-hop distance, thereby enhancing link feasibility and transmission efficiency. This repair strategy dynamically transforms the network topology, ensuring all quantum links remain within the physical limitations of the quantum channel while preserving network connectivity. The trusted node T serves as the primary repair candidate due to its central positioning and MDI-QKD capability, while quantum repeaters R provide alternative routing for geographically distributed user pairs. This hybrid approach extends the network's operational range beyond direct point-to-point quantum communication limitations, enabling scalable deployment over large scales. Direct communication among users is infeasible due to the limitations imposed by quantum channel losses and decoherence at long distances. Therefore, intermediary trusted nodes are required to facilitate secure and reliable communication. This network architecture enables the assessment of relay positioning efficiency, routing protocols, and secure key rate performance in practical long-distance quantum communication scenarios.

The physical layer of the hybrid quantum network employs MDI-QKD to achieve device independent security against detector side channel attacks. Each user terminal utilizes weak coherent pulse sources operating in the decoy state, where photon emission statistics follow a Poisson distribution as shown in Equation (3).

$$P(n \mid \mu) = \frac{\mu^n e^{-\mu}}{n!} \tag{3}$$

It represents the Poisson photon-number distribution, giving the probability of emitting n photons from a weak coherent source with mean photon number μ and is widely used in QKD systems to model practical laser sources. In MDI-QKD, quantum states from two users are transmitted to a central untrusted node for joint measurement. The conditional yield for an (n, m)-photon pair is given in Equation (4).

$$Y_{nm} = Y_{\text{photon}} + Y_{\text{dark}} + Y_{\text{baseline}}, \tag{4}$$

The overall yield Y_{nm} comprises three independent contributions as mentioned in Equation (5). photon-induced detections (Y_{photon}), false detections from detector dark counts (Y_{dark}), and baseline noise (Y_{baseline}). This decomposition enables accurate modeling of signal and noise effects in practical quantum communication systems.

$$Y_{\text{photon}} = p_{\text{BSM}} \left[1 - (1-\eta_A)^n\right] \left[1 - (1-\eta_B)^m\right], \tag{5}$$

$$Y_{\text{dark}} = p_{\text{dark}}(\eta_A + \eta_B), \quad Y_{\text{baseline}} = p_{\text{dark}}^2. \tag{6}$$

Y_{photon} gives the probability of successful Bell-state measurement from n and m photons arriving with channel efficiencies η_A and η_B, Y_{dark} models spurious detections due to single-detector dark counts and Y_{baseline} accounts for simultaneous dark counts, representing the system's constant background noise floor. This comprehensive yield model enables accurate estimation of MDI-QKD performance under practical experimental conditions, accounting for both signal dependent and signal-independent noise sources. The model provides the foundation for subsequent decoy-state analysis and SKR calculation within the optimisation framework. The decoy-state method includes the cornerstone of usable MDI-QKD performance, enabling rigorous analysis of single-photon parameters essential for unconditional security proofs. This technique employs multiple intensity levels, typically signal (μ), decoy (ν), and vacuum ($\omega = 0$) states to distinguish single-photon contributions from multi-photon components in the quantum channel.

$$Q_{ij} = \sum_{n,m=0}^{\infty} P(n|\mu_i) P(m|\mu_j) Y_{nm}, \tag{7}$$

The overall gain Q_{ij} is expressed in as the weighted sum of yields Y_{nm} over all photon-number pairs, where the weights correspond to the Poisson emission probabilities of sender and receiver with mean photon numbers μ_i and μ_j. In decoy state QKD protocols, such as decoy state BB84, security analysis depends on estimating the single-photon yield Y_{11} and single-photon error rate e_{11} to derive finite secret key rate bounds against eavesdropping as shown in Equation (9). The decoy state approach employs multiple signal intensities to statistically isolate multi-photon contributions, yielding tight bounds on these parameters. The observed gain Q_{ij} for intensity pair (μ_i, μ_j), where μ_i and μ_j denote the mean photon numbers of sender's and receiver's pulses where $P(n|\mu_i)$ represents the

Poisson probability of n photons given intensity μ_i, and Y_{nm} is the yield for n-photon pulses from sender and m-photon pulses from receiver. Similarly, the observed QBER E_{ij} for intensity pair (μ_i, μ_j) is given in Equation (8).

$$E_{ij} = \frac{\sum_{n,m=0}^{\infty} P(n|\mu_i)P(m|\mu_j)Y_{nm}e_{nm}}{Q_{ij}}, \tag{8}$$

where, e_{nm} denotes the error rate for the (n, m)-photon pair.

To ensure security, the lower bound on the single-photon yield Y_{11}^L is obtained via linear programming minimization under worst-case constraints from observed data:

$$Y_{11}^L = \min Y_{11}, \tag{9}$$

Equation (10). states that the observed gain Q_{ij} for intensity pair (μ_i, μ_j) is exactly reproduced by the weighted sum of photon-number yields Y_{nm}, where weights correspond to Poisson probabilities $P(n|\mu_i)$ and $P(m|\mu_j)$ for sender and receiver emitting n and m photons, respectively. The constraint ensures physical validity, as Y_{nm} represents the conditional detection probability given n and m photons sent, which must lie between 0 (no detection) and 1 (certain detection).

$$\sum_{n,m=0}^{\infty} P(n|\mu_i)P(m|\mu_j)Y_{nm} = Q_{ij}, 0 \leq Y_{nm} \leq 1 \tag{10}$$

The infinite summation is truncated to finite photon terms (e.g., $n, m \leq 3$ or higher, depending on intensities), as higher-order contributions become negligible due to the Poisson distribution tail. The upper bound on the single-photon error rate is given in Equation (11).

$$e_{11}^U = \frac{S_{11}^U}{Y_{11}^L}, 0 \leq e_{nm} \leq 0.5 \tag{11}$$

where, $S_{11}^U = \max(Y_{11}e_{11})$ is obtained via separate linear programming maximization, and Y_{11}^L is the previously computed single-photon yield lower bound. The asymptotic SKR for the MDI-QKD protocol is evaluated using :

$$R = P_Z \left[Y_{11}^L \left[1 - H_2(e_{11}^U) \right] - f_{\text{EC}} Q_{\mu\mu} H_2(E_{\mu\mu}) \right]^+, \tag{12}$$

where, $[x]^+ = \max(x, 0)$ ensures non-negativity. The term P_Z denotes the probability that sender and receiver select the Z-basis (key-generation basis), with successful Bell-state measurements. This expression formalizes the quantum communication trade off of information gain versus leakage cost. $Y_{11}^L[1 - H_2(e_{11}^U)]$ quantifies the secure information content from single-photon pair events, where Y_{11}^L is the lower bound on the conditional probability of successful Bell-state measurement given single-photon transmission by both parties, and e_{11}^U is the upper bound on the single-photon QBER. Thus, $H_2(e_{11}^U)$ quantifies the information per bit eavesdropper could possess about the key due to errors. f_{EC} quantifies the information cost of classical error correction efficiency. Here, $Q_{\mu\mu}$ is the success probability and $E_{\mu\mu}$ is the overall QBER, both measured in the key-generation basis. $H_2(E_{\mu\mu})$ approximates the minimum error-correcting information sender must publicly reveal to assist receiver's raw key correction. The efficiency factor $f_{\text{EC}} \geq 1$ accounts for non-ideal real-world error-correcting codes. This product is subtracted, as the disclosed information is fully accessible to eavesdropper. The binary Shannon entropy is defined in Equation (13).

$$H_2(x) = -x \log_2 x - (1 - x) \log_2(1 - x). \tag{13}$$

This measures the uncertainty of a binary random variable. Security is evaluated by modeling eavesdropping via degraded channel visibility and elevated error rates, testing R robustness against adversarial intervention. This determines tolerance thresholds such as maximum tolerable loss or QBER beyond which the key rate vanishes conclusively demonstrating the protocol's practical security limits. To overcome the computational complexity of global-scale MDI-QKD network design, a hybrid QIGA optimizes network topology. QIGA uses probabilistic qubit representation to efficiently explore a huge configuration space, compared to classical GAs, which employ deterministic binary strings. Every network topology is preserved as a multiqubit quantum chromosome. Mathematical representation of qubit [42], is represented in Equation (14).

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1, \tag{14}$$

where, $|0\rangle$ and $|1\rangle$ signify mathematical basis states, and the complex values α and β relate to standardization constraints. This superposition enables simultaneous encoding of both binary states (0 and 1) with probabilities $|\alpha|^2$ and $|\beta|^2$. For topology optimization, each qubit represents link presence / absence or node type assignment, allowing parallel representation of multiple configurations. During evaluation, each qubit undergoes quantum measurement, collapsing probabilistically into a classical binary value (0 or 1) according to squared amplitude magnitudes $|\alpha|^2$ and $|\beta|^2$. This yields a classical chromosome instance for fitness assessment, incorporating metrics from prior particularly total SKR (summed across user pairs), network cost, and physical-layer constraints. To evolve the population toward optimal solutions, quantum chromosomes are updated via quantum rotation gates. For a single qubit, the update applies the rotation matrix as given in Equation (15):

$$\begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \tag{15}$$

where, θ is the rotation angle, with magnitude and sign adaptively determined from current solution fitness and the global best. This systematically adjusts probability amplitudes to favor high-fitness configurations in subsequent measurements. To mitigate premature convergence, stagnation detection monitors fitness progress across generations. Upon identifying a converged defined by a threshold number of iterations without improvement, systematically increases the rotation angle magnitude $|\theta|$ to amplify exploration and diversify the quantum population. A key physical constraint in quantum networks is the maximum transmission distance $d_{\max}$, beyond which channel loss renders secure key distribution infeasible.

The process concludes by using a broad multi-criteria decision framework to assess QIGA's solutions and confine the optimum hybrid quantum network topology. This is feasible because a weighted fitness function balances efficiency,

security, physical accessibility, and economic viability. The fitness F of a candidate network topology is computed as Equation (16).

$$F = w_1 \log_{10}(R_{\text{avg}}) - w_2 \cdot \text{QBER}_{\text{pen}} - w_3 \cdot L_{\text{norm}} - w_4 \cdot C_{\text{norm}} \tag{16}$$

where $w_1, w_2, w_3, w_4 > 0$ are weighting coefficients reflecting design objective priorities with $\sum w_i = 1$. Performance Factor ($w_1 \log_{10}(R_{\text{avg}})$) main goal is to optimize the network's operational throughput.

R_{avg} denotes the average secret key rate per user pair. The average key rate R_{avg} against penalties from the QBER, transmission loss, and system cost., as shown in Equation (17).

$$\text{QBER}_{\text{pen}} = \sum_i \max(0, E_i - E_{\text{th}})^2, \tag{17}$$

The $QIGA{-}OT$ encourages to improve the fitness function F as effective as it can be. The candidate topology that yields the maximum F post-convergence is selected as the optimal hybrid quantum network architecture. This thorough evaluation framework ensures that the final design meets the requirements of high key generation, unconditional security, technical feasibility, and cost efficiency at the same time. This enables global quantum network scaling.

MQE is utilized to assess the efficiency of each communication channel. This statistic encompasses numerous essential parameters, including the SKR, QBER, overall signal attenuation, and connection cost. The allocation of each component's contribution to the MQE score is weighted as detailed as follows: 50% is assigned to SKR, reflecting its primary importance; 20% to QBER; 25% to signal loss; and the remaining 5% to link cost.

The introduction of quantum repeaters, while essential for enabling long-distance communication, inevitably increases system complexity and deployment cost. To account for this effect, the weight assigned to the link cost metric is elevated. Specifically, when a single repeater is employed, the cost weight is increased to 7%. After normalizing the weights to ensure a total of 100%, the adjusted values are obtained as 49.02% for SKR, 19.61% for QBER, 24.51% for channel loss, and 6.86% for link cost.

Fig. 2 illustrates an effective optimization technique as QIGA used for a robust quantum communication network. The proposed QIGA initializes qubits in equal superposition using hybrid topology connections and quantum chromosomes. This method minimizes communication losses and maximizes SKR in QKD systems due to topological and physical restrictions. A network topology is uniquely represented by each QIGA candidate solution in the optimization framework. By iteratively finding the shortest links, the quantum initialization method creates population ring pathways with near optimum cycles. Low-loss initial solutions, reduced channel loss, and reduced quantum repeater reliance result from this initialization.

For each communication link, essential parameters such as distance, optical loss, QBER and SKR are evaluated based on the BB84 protocol. These parameters are then integrated into a unified performance measure, termed as MQE, which incorporates SKR, QBER, total channel loss, and link cost. This metric

Algorithm 1 QIGA-Based Hybrid MDI QKD Network Optimization with Trusted Node and Repeaters

Input: Number of users U, deployment area $A \times A$, maximum link distance $D_{\max}$, QIGA parameters $(P, G, \theta_{\min}, \theta_{\max})$,
MDI-QKD physical parameters $\{\alpha, \eta_d, p_{\text{dark}}, \mu, \nu, f_{\text{ec}}\}$.
Output: Optimized hybrid topology T; best fitness value F

STEP 1: INITIALIZE USER SET $\mathcal{U} = \{u_1, \ldots, u_U\}$ UNIFORMLY AT RANDOM IN THE DEPLOYMENT AREA $A \times A$
Place trusted node T at the geometric center of the deployment area $A \times A$
Compute distances d_{ij}; insert repeaters $\mathcal{R}$ for $d_{ij} > D_{\max}$
Compute pairwise distances $d_{ij} = \|\mathbf{x}_i - \mathbf{x}_j\|_2$
Insert repeater nodes $\mathcal{R}$ for all pairs (i, j) with $d_{ij} > D_{\max}$
Encode each candidate topology as a quantum chromosome of length N_q

STEP 2: QUANTUM POPULATION INITIALIZATION
Initialize $|\psi^{(0)}\rangle = \bigotimes_{k=1}^{N_q} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$g \leftarrow 1$, $F^\star \leftarrow -\infty$
while $g \le G$ **do**
Measure each quantum chromosome to obtain a binary population
Decode each chromosome into a hybrid topology (ring/star/mesh) links
for each link (i, j) **do**
if $d_{ij} \le D_{\max}$ **then**
Retain direct link
else
Select intermediate node $k \in \{T\} \cup \mathcal{R}$ s.t. $d_{ik} \le D_{\max},\ d_{kj} \le D_{\max}$
end if
end for
STEP 3: EVOLUTIONARY OPTIMIZATION
Evaluate each MDI-QKD link (i, k, j)
Compute channel transmittances:
$\eta_i = \eta_d 10^{-\alpha d_{ik}/10}$, $\eta_j = \eta_d 10^{-\alpha d_{kj}/10}$
Estimate $Q_{\mu_a \mu_b}$, $E_{\mu_a \mu_b}$; bound Y_{11}^L, e_{11}^U via decoy-state LP
Compute secret key rate
$R = P_Z[Y_{11}(1 - H_2(e_{11})) - f_{\text{ec}} Q_{\mu\mu} H_2(E_{\mu\mu})]$
Aggregate average SKR $\bar{R}$, average QBER $\bar{e}$, average loss $\bar{L}$, and cost C
Compute fitness
$F = w_1 \log(\bar{R}) - w_2 \bar{e} - w_3 \bar{L} - w_4 C$
if $F > F^\star$ **then**
$F^\star \leftarrow F$, $\mathcal{T}^\star \leftarrow$ current topology
end if
Update quantum amplitudes toward the best solution:
for each qubit $k = 1$ **to** N_q **do**
$\begin{bmatrix} \alpha_k' \\ \beta_k' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \alpha_k \\ \beta_k \end{bmatrix}$
end for
Adapt rotation angle θ dynamically based on convergence behavior
STEP 4: RETURN OPTIMIZED SOLUTION
return $\mathcal{T}^\star$, $F^\star$

provides a comprehensive benchmark for assessing network quality and supports the design of scalable, high-performance quantum networks suitable for practical deployment.

The process of identifying significant metrics for each individual link is detailed, and the resulting data are aggregated to evaluate the system as a whole. It calculates the overall signal attenuation, the average SKR, QBER, and the total expense of the links. Employing these factors, it computes MQE, a composite metric that evaluates the trade-offs between security, efficiency, and infrastructure costs. This comprehensive methodology enables a precise assessment of the network's effectiveness for quantum-secure transmission. Sum of all link loss implies cumulative signal degradation. Averaging the SKR and QBER values over all established links gives an overall assessment of secure key generation efficiency and communication dependability. The link cost comprises the network complexity, which is the total amount of links plus twice the number of repeaters.

$$\text{MQE} = w_1 \cdot \text{avg\_skr} - w_2 \cdot \text{avg\_qber} - w_3 \cdot \text{total\_loss} - w_4 \cdot \text{link\_cost} \tag{18}$$

MQE analyzes network quality by focusing enhanced

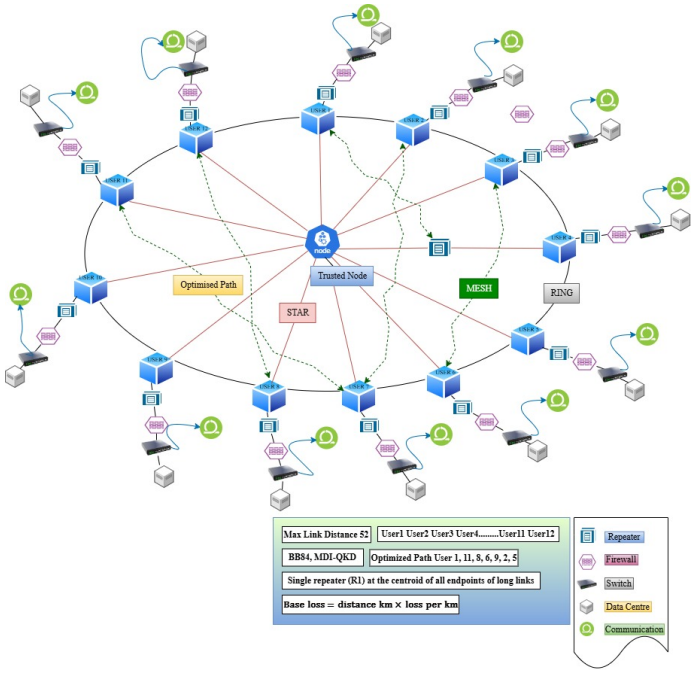

Fig. 2. The visualization of a Hybrid Quantum Network framewok optimized by Quantum inspired genetic algorithm(QIGA): A Quantum-Inspired Genetic Algorithm (QIGA) enhances a centrally located trusted node (T), a shared repeater (R1), and a quantum network with 12 users. The hybrid topology enhances Secure Key Rate (SKR) and robustness by using dashed mesh links for optimal redundancy, red star links for central communication via T, and black ring links for cyclic connectivity. QIGA optimizes the Merit of Quantum Efficiency (MQE) by removing extended linkages through R1 and establishing robust mesh connections by achieving a balance between exploration and utilization. To improve security and resilience, each user is linked to an individual repeater, switch, firewall, data center, and communication line.

TABLE I
COMPARISON OF OPTIMIZED TOPOLOGIES (EAVESDROP=TRUE AND EAVESDROP=FALSE)

Optimized Topology (Eavesdrop=True)					**Optimized Topology (Eavesdrop=False)**				
Link	Distance (km)	Loss (dB)	QBER	SKR (bits/s)	Link	Distance (km)	Loss (dB)	QBER	SKR (bits/s)
R1-User10	9.39	1.878	0.1243	4.65e-04	R1-User10	9.39	1.878	0.0325	1.13e-03
R1-User4	21.40	4.280	0.1250	2.64e-04	R1-User4	21.40	4.280	0.0327	355.34
R1-User5	17.71	3.542	0.1248	3.14e-04	R1-User5	17.71	3.542	0.0327	7.65e-04
T-User11	17.61	3.522	0.1248	3.16e-04	T-User11	17.61	3.522	0.0327	7.68e-04
T-User8	16.88	3.377	0.1247	3.27e-04	T-User8	16.88	3.377	0.0327	7.95e-04
User1-User7	37.23	7.446	0.1256	1.26e-04	User1-User7	37.23	7.446	0.0330	3.09e-04
User1-User9	24.81	4.961	0.1251	2.25e-04	User1-User9	24.81	4.961	0.0328	5.50e-04
User10-User11	25.90	5.181	0.1252	2.14e-04	User10-User11	25.90	5.181	0.0328	5.23e-04
User10-User2	48.51	9.702	0.1261	7.42e-05	User10-User2	48.51	9.702	0.0333	1.83e-04
User10-User5	9.46	1.892	0.1244	4.64e-04	User10-User5	9.46	1.892	0.0325	1.12e-03
User10-User7	33.80	6.760	0.1255	1.48e-04	User10-User7	33.80	6.760	0.0330	3.63e-04

SKR and diminished QBER, loss, and expense. where w_1, w_2, w_3, w_4 are predefined weights that represent the relative significance of each factor as shown in Equation 18. This transformation reduces the complexity of the optimization process by reformulating the inherently multi-objective problem into a single-objective framework. Facilitating direct optimization while incorporating the relative significance of each contributing factor. The quantum communication network structure is optimized using QIGA as shown in Algorithm 1. QIGA integrates with a MDI-QKD physical layer to optimize the topology of a hybrid quantum communication network. The network comprises end-users, quantum repeaters, and a central trusted node. The main objective is to maximize the SKR, minimizing the QBER, channel loss, and cost. Initially, the algorithm deploys U_U end-users uniformly at random within a square area of size $A \times A$ and positions the trusted node at the center. Quantum repeater nodes are inserted along links exceeding the maximum permissible distance $D_{\max}$, ensuring hardware-compliant connectivity. Candidate network topology is then encoded as a quantum chromosome, represented by a string of N_q qubits with probability amplitudes α_k and β_k that determine the collapse probabilities to states 0 or 1.

In quantum population phase, the algorithm initializes a population of quantum chromosomes by setting each qubit to the uniform superposition state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. This superposition ensures equal probability for all classical binary strings upon measurement, enabling quantum parallelism to represent a vast space of candidate network topologies. Concurrently, the generation counter g is set to 1 and the global best fitness value $F^\star$ is initialized to $-\infty$, preparing the system for iterative optimization. Topologies are validated by retaining direct links

only if the node distance $d_{ij} \leq D_{\max}$; otherwise, feasible two-hop MDI-QKD links are constructed via intermediate nodes satisfying distance constraints. Fitness is evaluated using a comprehensive MDI-QKD model: for each link (i, k, j), channel transmittances η_i and η_j are computed, decoy-state analysis via linear programming provides bounds Y_{11}^L and e_{11}^U, and the secret key rate R_{ij} is derived. Network-level metrics average SKR $\bar{R}$, QBER $\bar{e}$, loss $\bar{L}$, and cost C are aggregated into the weighted fitness function $F = w_1 \log(\bar{R}) - w_2\bar{e} - w_3\bar{L} - w_4 C$. Superior solutions update the global best $F^\star$. The quantum population evolves via rotation gates, where each qubit state $[\alpha_k, \beta_k]^T$ rotates by angle θ_k, dynamically biasing amplitudes toward elite solutions. Upon completion of G generations, the algorithm terminates and outputs the optimized hybrid network topology $T^\star$ and its corresponding maximum fitness value $F^\star$. This solution optimally balances high secret key rate, low quantum bit error rate, minimal channel loss, and deployment cost. The key innovation lies in the joint optimization of network topology and MDI-QKD physical parameters. The QIGA framework enables efficient global exploration of the large discrete solution space, while the integrated decoy-state MDI-QKD model ensures physically realistic and secure designs against practical attacks.

QIGA simulates quantum parallelism using a population-centric optimization method, where in greedy initialization prioritizes shorter-distance connections. The implementation of a ring topology ensures complete network connectivity, making very appropriate for QKD systems. The fitness function, grounded in the MQE, equilibrates security (minimizing QBER), performance (maximizing SKR), and resource efficiency (minimizing optical loss and link cost). To evaluate topology, the function is intended to determine the performance of a specified network architecture under eavesdropping and normal, as shown in Table I. For every link between two nodes, the function computes the physical distance using a pre-computed matrix. SubsequentLy, by using the BB84 protocol, the function evaluates the QBER and SKR. The hybrid topological framework integrates mesh (short secure links), ring (cyclic connectivity), and star (centralized via T) to enhance the secure key rate and resilience. The optimized hybrid topology, comprising 22 links, demonstrates robust performance under normal channel conditions while revealing characteristic vulnerabilities in the presence of an eavesdropper. These results validate the hybrid architecture's high key rates and low QBER in trusted environments while demonstrating the expected security compromise against active interception. Thus emphasizing the significance of constant monitoring and post-processing improvements for practical implementation.

QIGA offers significant advantages over conventional GA for optimizing hybrid MDI-QKD network topologies. Unlike GA's fixed binary or real-valued chromosomes with random crossover and mutation, QIGA employs probabilistic qubits in superposition, enabling a single individual to encode multiple solutions simultaneously and achieving exponentially higher population diversity with fewer individuals. This approach facilitates more thorough exploration of complex, multimodal search spaces. Additionally, QIGA utilizes quantum rotation gates for deterministic, guided updates of probability amplitudes toward optimal solutions, providing superior exploration-exploitation balance, faster convergence, and reduced risk of premature local optima entrapment compared to GA's stochastic operators. Consequently, QIGA delivers superior solution quality in fewer generations for multi-objective optimization of secret key rate, error rate, loss, and cost. The method reduces the need for broad links through R1 and increases reliability via mesh connections.

IV. Performance Evaluation

A. Experimental setup

The experiment model a quantum network that includes a hybrid topology, optimized via QIGA. We have proposed a model in Python 3.10 utilizing Matplotlib on a system using an Intel(R) Xeon(R) Gold 6248R CPU operating at a speed of 3.00 GHz (with 2 processors) and 128GB of RAM. The system operates on a 64-bit operating system and utilizes Python version 3.12.4. The experimental setup simulated a quantum network over a 100×100 km area with 12 user nodes randomly placed, one central trusted node T at the centroid (50,50) km. A single shared repeater R1 dynamically positioned at the centroid of 3 identified long links exceeding 52 km to minimize infrastructure while segmenting distances.

The QIGA-optimized hybrid MDI-QKD topology derived using 100 generations and a population size of 40. Decoy-state MDI-QKD parameters comprised 0.2 dB/km loss, 10% detector efficiency, and eavesdropping simulated at 0.85 visibility. As detailed in Table IV, the topology features 22 links, with a total loss of 99.41 dB. Under normal conditions, it yields an average SKR of 7.16×10^{-4} bits/pulse, QBER of 0.054, and MQE of 2.265. Under eavesdropping, the SKR decreases by 58.7% to 2.96×10^{-4} bits/pulse, QBER increases to 0.125, and MQE drops to 2.067, while maintaining positive key rates network-wide. Visualizations in Fig. 6, reveal 77% direct high-performance links (dark green) under normal conditions, with degradation to orange/red under attack. The optimized ring path clusters short distances effectively while routing longer paths through infrastructure, underscoring the framework's robustness for secure, efficient metropolitan-scale quantum networks under adversarial conditions.

Fig. 3 shows how the proposed $QIGA - OT$ approaches convergence. It shows how the best fitness value changes over 100 generations. The blue line illustrates the highest fitness level reached in each generation. The red dashed line shows a moving average (with a window size of about 5 to 10 generations) to show the overall pattern and balance out short-term changes. The multi-objective fitness function maximizes the average SKR per pulse while assessing higher QBER, channel loss, and infrastructure costs related to links, trusted nodes, and repeaters. Greater values mean better network performance and efficiency. Such a convergence design shows that the QIGA is efficient for the complex search space of hybrid quantum network topology optimization.

B. Result Analysis

In this section, we describe the result of the simulation of the proposed quantum network framework. A total of 14

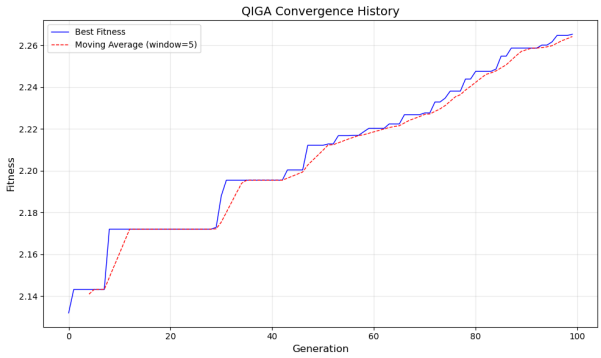

Fig. 3. Convergence history of the proposed QIGA illustrating optimization performance for hybrid MDI-QKD network.

TABLE II
RING TOPOLOGY

Condition	Links	Total Loss (dB)	Avg SKR (bits/s)	Avg QBER	MQE
Ring (Normal)	13	61.55	6.05e-04	0.0328	2.546695
Ring (Eavesdrop)	13	61.55	2.48e-04	0.1251	2.327118

nodes are placed throughout a 100×100 km area for the experiments, which included 12 user nodes, one trusted node T and one repeater $R1$. After 52 km, $R1$ is used to segment long links. This is the maximum link distance. In terms of ensuring connectivity, this shared repeater strategy reduced infrastructure overhead. We evaluated the performance and security trade offs in quantum communication networks by optimizing three topologies with a QIGA: ring, ring-star, and ring-star-mesh hybrid.

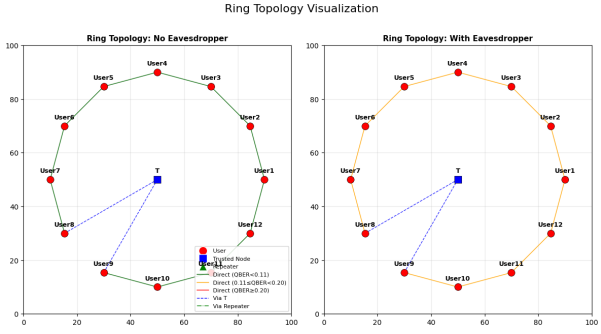

Fig. 4. Visualizing Optimized Ring Topologies of a multi-user quantum network (Green Link: direct QKD connection, Red Dot: User, R1: Repeater, Blue Dot: Trusted Node, Dashed blue link: communication established via the trusted)

The performance summary of the ring topology network is evaluated under both normal and eavesdropper conditions as shown in Fig. 4. The optimized architecture employs a pure ring structure with 13 direct trusted-node (T) links: 11 links constitute the primary ring, augmented by 2 shortcut T-links to improve connectivity and overall performance as shown in Table II. The design eliminates the need for quantum repeaters or repeater links, prioritizing simpler direct transmission paths to minimize hardware complexity and deployment costs. Optimized ring ordering is User3 → User4 → User5 → User6 → User7 → User8 → T → User9 → User10 → User11 → User12 → User1 → User2.

The physical infrastructure remains unchanged across both scenarios, maintaining a constant total channel loss of 61.55 dB. Under normal scenario, the network achieves a higher average SKR of 6.05×10^{-4} bits per pulse and a low QBER of 3.28%. In the adversarial scenario, the SKR decreases to 2.48×10^{-4} bits per pulse, while the QBER rises to 12.51%. This degradation aligns with QKD security proofs, where eavesdropping induces detectable errors, thereby reducing the secure key rate.

These results demonstrate the optimized ring topology's capacity to balance key generation efficiency, security, and resource utilization, while clearly quantifying the performance penalty from eavesdropping.

However, it is free of redundancy, which makes it less versatile. The network serves best when it is secure, which shows that QIGA can create strong quantum topologies that preserve data safe. The network's different levels of performance show how important it is to optimize topology, trusted repeaters, and routing in order to minimize eavesdropping and maximize SKR.

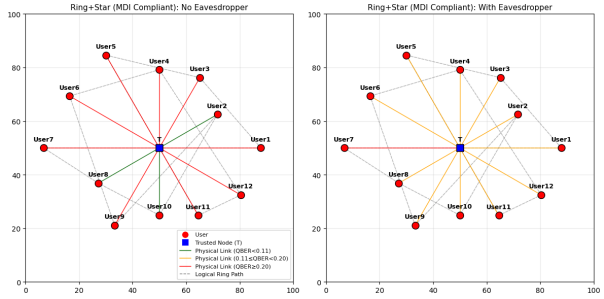

Fig. 5. Visualizing Optimized Ring-Star Topologies of a multi-user quantum network (Green Link: Physical link, Red Dot: User, Blue Dot: Trusted Node, Dashed blue link: Logical ring path)

The ring-star topology as shown in Table III, utilizes a fully connected ring-star physical infrastructure with all users directly linked to T. Comprising 12 physical links, total channel loss of 78.67 dB, and infrastructure cost of 12.0. Under normal conditions, this yields an average SKR of 3.38×10^{-5} bits/pulse with QBER of 38.33%. These results demonstrate the topology's simplicity and connectivity advantages using only T, yet highlight inferior key rates versus hybrid designs leveraging direct short-distance links. Logically, these connections support a 12 edge ring pattern (User1 → User3 → User5 → User11 → User12 → User4 → User6 → User9 → User2 → User10 → User8 → User7), enabling pairwise key distribution via T.

Fig. 5 illustrates the physical and logical structure of the corrected ring-star topology, fully compliant with MDI QKD requirements. Users appear as red circles arranged approximately in a ring around T, depicted as a blue square at the network. Solid lines represent physical quantum links (user to T), colored by QBER: dark green for QBER < 0.11 (secure, high-performance), orange for $0.11 \leq$ QBER < 0.20

TABLE III
(RING+ STAR) TOPOLOGY

Condition	Links	Total Loss (dB)	Avg SKR (bits/s)	Avg QBER	MQE
Hybrid (Normal)	24	78.67	3.38e-05	0.3833	1.265285
Hybrid (Eavesdrop)	24	78.67	3.14e-05	0.1582	1.813768

TABLE IV
OPTIMISED TOPOLOGY (RING+STAR+MESH)

Condition	Links	Total Loss (dB)	Avg SKR (bits/s)	Avg QBER	MQE
Hybrid (Normal)	22	99.41	7.16e-04	0.054	2.265209
Hybrid (Eavesdrop)	22	99.41	2.96e-04	0.125	2.066849

(marginally secure), and red for QBER ≥ 0.20 (high error rate). Dashed gray lines overlay the logical ring communication path, showing the optimized cyclic order (User1 $\rightarrow$ User3 $\rightarrow$ User5 $\rightarrow \ldots \rightarrow$ User7 $\rightarrow$ User1), with each logical user-user connection realized via two physical segments through T performing Bell-state measurements. The visualization confirms no direct user-to-user quantum channels all communication routes through T, ensuring MDI-QKD security against detector-side attacks. Under eavesdropping, several physical links shift to orange/red due to elevated error rates, yet the topology remains unchanged for direct security degradation assessment. This design achieves simplicity, full connectivity, and MDI compliance with only 12 physical links and no repeaters, with lower average SKR versus hybrid topologies incorporating direct short distance connections.

The hybrid topological framework as shown in Table IV. comprises 22 links (17 direct user-to-user, 2 via central trusted node T, 3 via single midpoint repeater), achieving identical total channel loss of 99.41 dB and infrastructure cost of 26.0 across both scenarios. Under normal conditions, the network delivers an average SKR of 7.16×10^{-4} bits/pulse with QBER of 0.054 (below the 0.11 security threshold). An intercept-resend attack (Eve visibility = 0.85) reduces SKR by 58.7% to 2.96×10^{-4} bits/pulse while elevating QBER to 0.125 still within secure bounds of decoy-state MDI-QKD. MQE declines from 2.265 to 2.067, yet maintains positive key rates network-wide.

In conclusion, the ring topology is more efficient for SKR, but it is less reliable. The hybrid topology can handle wider networks, but there is more loss. The ring-star topological framework is the best setup because it strikes the best balance between key rate, error resilience, eavesdropping detection, and network scalability. QIGA-optimized hybrid network topology visualizes in Fig. 6, with normal and eavesdropper scenarios. Users appear as red circles, the central trusted node (T) as a blue square at the centroid (50, 50 km), and the single repeater (R1) as a green triangle at the midpoint of the longest user pair. Quantum links are distinguished by different color and style, solid dark green for direct user-to-user links with QBER < 0.11 (high-performance, secure),

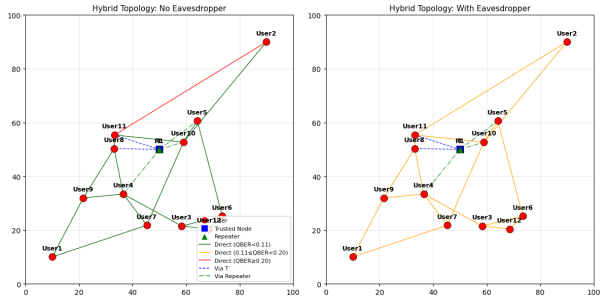

Fig. 6. Visualizing Optimized Ring-Star-Mesh Topologies (Green Link: Direct link, Red Dot: User, Blue Dot: Trusted Node, Dashed blue link: via Trusted node)

solid orange for $0.11 \leq$ QBER < 0.20 (marginally secure), solid red for QBER ≥ 0.20 (low key rate), dashed blue for T routed paths, and dash-dotted green for repeater-assisted connections. The visualization reveals that 77% of the 22 links are direct high performance (dark green) connections, demonstrating the optimizer's prioritization of short, low-loss paths to maximize SKR, while the trusted node and single repeater ensure full connectivity for longer distances with minimal infrastructure overhead. The topology remains identical across both scenarios, enabling direct performance comparison under eavesdropping attack conditions, where several direct links degrade from dark green (QBER < 0.11) to orange/red (QBER ≥ 0.11) due to elevated QBER. Nevertheless, positive secret key rates are maintained network-wide. This spatial visualization demonstrates the robustness of the hybrid topology, leveraging strategic trusted node placement and limited repeater deployment for scalable MDI-QKD networks.

The research analysis illustrates that while expanding network connectivity, redundancy, and resilience, increasing topology issues from ring to hybrid causes more links and overall channel loss. The ring topology has the lowest loss and the highest key rate, but it lacks fault tolerance and scalability. Better SKR performance, lower QBER, and increased robustness are all balanced by hybrid topologies. As evidenced by the constant rise in QBER and fall in SKR during an attack, the QIGA-based optimization precisely identifies the best routes that preserve security under typical circumstances and respond to eavesdropping. MQE trends further indicate that hybrid topologies are highly suitable for real quantum networks since they grow safely while preserving effective key distribution.

Fig. 7 shows the SKR distribution for the links in the optimized hybrid topology, classified by types of link, Direct user, Via T (user-to-trusted node-to-user for MDI-QKD), and Via Repeater (user-to-repeater-to-user for long-distance links that extend over the maximum direct link threshold). It clearly displays that there is a strong connection between the type of link and the performance of key generation. This directly reflects the physical channel characteristics in MDI-QKD. SKR distribution across link types in the QIGA-optimized topology reveals a distinct performance hierarchy driven by channel attenuation. Direct user links exhibit the highest SKR with the widest variance due to varying distances (≤ 52 km).

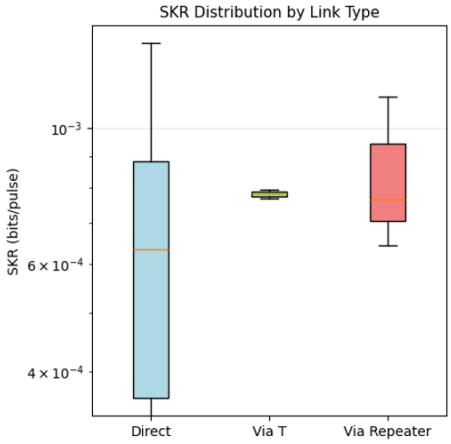

Fig. 7. SKR distributions for different infrastructure assisted links in a QIGA optimized hybrid network, illustrating the trade-off between connectivity and key generation efficiency.

Links routed through T demonstrate superior performance and reduced variability, enabled by symmetric channel splitting via Bell-state measurement at T. Repeater-assisted links yield the lowest SKR, attributable to longer individual segments despite midpoint repeater placement. Compared to the fully connected time-bin-entangled network [10], our proposed hybrid optimised topology of quantum network exhibits a number of significant benefits. This network is optimized using QIGA with shared repeaters and BB84 MDI-QKD as shown in Table VI.

We analyze the results of multi-objective optimization for a QKD network in Table V, performed via a QIGA coupled with a weighted sum method. The formulation optimizes five objectives: maximization of SKR, enhancement of security via minimization of QBER, cost minimization, QBER reduction, and overall loss. These objectives exhibit inherent trade-offs for instance, denser connectivity boosts SKR but elevates cost and QBER due to extended link lengths. Multi-objective optimization thus yields a Pareto front of non-dominated solutions, enabling designers to select configurations tailored to mission-specific priorities. To find the best trade-offs, multi-objective optimization is essential. It give users a set of approaches that are not determined by others, so they can choose configurations based on their own requirements. The multi-objective optimization gave a range of reliable limits, with three extreme solutions that show important trade-offs in the hybrid MDI-QKD network. The SKR-maximizing solution reached the highest secret key rate of 4.67×10^{-4} bits/pulse through a dense network of 53 links (39 direct, 8 trusted-node-routed, and 6 repeater-routed). However, it also cost the most (60 units) and had the highest QBER (0.0858), which was caused by a lot of channel losses and interference across many or long pathways.

Cost-minimized configuration utilized the fewer links (42 with 37 direct, 2 via the trusted node, and 3 via the repeater), achieving the lowest deployment cost of 46 units.

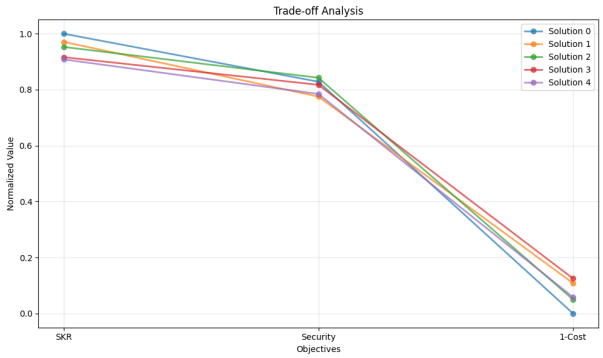

Fig. 8. Performance trade-offs and optimal solutions from multi-objective QIGA optimization

However, this resulted in degraded performance, with an SKR of 4.12×10^{-4} bits/pulse and the highest QBER of 0.0885, attributable to heavy reliance on lossy direct channels and limited relay support. The optimized solution, providing the minimum QBER of 0.0787, achieved an intermediate balance with an SKR of 4.45×10^{-4} bits/pulse and a cost of 57 units across 51 links (36 direct, 6 via the trusted node, and 9 via the repeater). This demonstrates that intensive repeater utilization effectively suppresses transmission errors at moderate additional cost and minimal SKR penalty. These extremes collectively highlight the inherent trade-offs among throughput, security, and deployment cost, underscoring the value of the proposed multi-objective QIGA framework for generating application specific quantum network.

Fig. 8, illustrates the performance trade-offs among five optimal solutions via a normalized line plot, with each objective scaled to the range $[0, 1]$ for equitable comparison. The x-axis categorizes the three objectives (SKR, security, and inverted cost labeled as "1-Cost") which represent normalized secret key rate (SKR, higher better), normalized security (inverse QBER, higher indicates lower error rate), and normalized inverse cost (higher indicates lower deployment cost). The y-axis depicts normalized performance from 0 to 1 (higher values indicate superior performance for all objectives). Each colored line connects the performance values of one solution across these dimensions, forming unique profiles. For instance, the maximum SKR solution achieves peak performance on the SKR axis but underperforms in security and inverse cost, while the cost-optimized solution excels in inverse cost at the expense of SKR and security. The security optimized solution exhibits a balanced profile with high security, respectable SKR, and moderate cost. It further makes it easy for users to select a network topology that meets their needs, such as increasing throughput, making the network more resistant to errors, or lowering infrastructure costs in real-world MDI-QKD deployments.

V. Conclusions And Future Work

Our proposed framework demonstrates the effectiveness of QIGA for optimizing a hybrid topology for scalable MDI-QKD networks. By integrating a trusted node for Bell-state measurements and deploying a shareble quantum repeater at

TABLE V
OPTIMAL SOLUTIONS FROM MULTI-OBJECTIVE QIGA OPTIMIZATION

Solution Type	SKR (bit\pulse)	QBER	Total Cost (units)	Total Links	Direct Links	Via T	Via R1
Best SKR	4.67×10^{-4}	0.0858	60.0	53	39	8	6
Best Cost	4.12×10^{-4}	0.0885	46.0	42	37	2	3
Best Security (Lowest QBER)	4.45×10^{-4}	0.0787	57.0	51	36	6	9

TABLE VI
COMPARISON TABLE WITH PROPOSED TECHNIQUE

Topology	Mesh [9]	Fully Connected [20]	Fully Connected [27]	QIGA-OT Hybrid (Proposed)
Scalability	Moderate	Low	Moderate	High
Repeaters/ Trusted Nodes	No repeaters, multi-hop trusted nodes	No repeaters & trusted nodes	No repeaters, trusted node free	1 Shared repeater & 1 Trusted node
SKR	_	∼300-500 bits/s	∼200-300 bits/s	∼716e-04 bits/s (normal), ∼2.96e-04 bits/s (eavesdrop)
QBER	_	∼0.05-0.10 %	∼0.08-0.12 %	∼0.054 (normal), ∼0.125 (eavesdrop)
System Loss	Low (∼10-20 dB per hop, multi-hop increases)	Moderate (∼20-30 dB)	Moderate (∼15-25 dB)	∼99.41 dB
Resource Efficiency	–	Quadratic (120 pairs for 16 users)	Quadratic (28 pairs for 8 users)	Subquadratic (∼19 links + 3 repeater)
Eavessdrop (Proposed)	–	–	–	QBER drop ∼56.8%; SKR rises ∼141.8%
MQE (Proposed)	–	–	–	∼2.265 (superior SKR, low QBER);

the midpoint of the longest user separation and full connectivity is achieved. While automatically repairing long-distance connections exceeding 52 km. The optimized topology attains a high average SKR of 7.16×10^{-4} bits/pulse with a low QBER of 0.054 under normal operating conditions, and it maintains positive key generation under strong intercept-resend eavesdropping (SKR = 2.96×10^{-4} bits/pulse, QBER = 0.125; 58.7% SKR degradation). The multi-objective quality estimate improves from 2.067 (adversarial) to 2.265 (normal), indicating a favorable balance among key rate, security, overall channel loss (99.41 dB total), and infrastructure cost. Future research directions include the refinement of the quantum repeater model to eliminate simulation artifacts and the incorporation of realistic eavesdropping strategies, such as photon-number-splitting attacks, to enhance security evaluation. Additionally, the exploration of multi-repeater configurations is anticipated to improve the scalability of quantum key distribution networks. The integration of dynamic noise models and the consideration of inherent fiber imperfections are expected to further strengthen the applicability of the proposed framework under practical deployment scenarios. Furthermore, extending the QIGA to support hybrid network topologies offers provide additional optimization opportunities for achieving higher performance and scalability.

REFERENCES

[1] Gisin, N. and Thew, R., 2007. Quantum communication. Nature photonics, 1(3), pp.165-171.

[2] Yang, Z., Zolanvari, M. and Jain, R., 2023. A survey of important issues in quantum computing and communications. IEEE Communications Surveys & Tutorials, 25(2), pp.1059-1094.

[3] Elliott, C., 2002. Building the quantum network. New Journal of Physics, 4(1), p.46.

[4] Runser, R.J., Chapuran, T., Toliver, P., Peters, N.A., Goodman, M.S., Kosloski, J.T., Nweke, N., McNown, S.R., Hughes, R.J., Rosenberg, D. and Peterson, C.G., 2007. Progress toward quantum communications networks: opportunities and challenges. Optoelectronic Integrated Circuits IX, 6476, pp.147-161.

[5] Lee, Y., Dai, W., Towsley, D. and Englund, D., 2024. Quantum network utility: A framework for benchmarking quantum networks. Proceedings of the National Academy of Sciences, 121(17), p.e2314103121.

[6] Hildebrand, B., Ghimire, A., Amsaad, F., Razaque, A. and Mohanty, S.P., 2023. Quantum communication networks: Design, reliability, and security. IEEE Potentials, 44(1), pp.4-10.

[7] Valls, V., Promponas, P. and Tassiulas, L., 2024. A Brief Introduction to Quantum Network Control. IEEE Communications Magazine, 62(10), pp.48-53.

[8] Khan, M.A., Ghafoor, S., Zaidi, S.M.H., Khan, H. and Ahmad, A., 2024. From quantum communication fundamentals to decoherence mitigation strategies: Addressing global quantum network challenges and projected applications. Heliyon, 10(14).

[9] McClean, J.R., Kimchi-Schwartz, M.E., Carter, J. and De Jong, W.A., 2017. Hybrid quantum-classical hierarchy for mitigation of decoherence and determination of excited states. Physical Review A, 95(4), p.042308.

[10] Chiti, F., Picchi, R. and Pierucci, L., 2024. A survey on non-terrestrial quantum networking: Challenges and trends. Computer Networks, 252, p.110668.

[11] Lo, H.K., Curty, M. and Qi, B., 2012. Measurement-device-independent quantum key distribution. Physical review letters, 108(13), p.130503.

[12] Zhang, Y. and Ni, Q., 2018, August. Design and analysis of secure quantum network system with trusted repeaters. In 2018 IEEE/CIC International Conference on Communications in China (ICCC) (pp. 511-514). IEEE.

[13] Perseguers, S., Lewenstein, M., Acín, A. and Cirac, J.I., 2010. Quantum random networks. Nature Physics, 6(7), pp.539-543.

[14] Gao, X.Q., Zhang, Z.C. and Sheng, B., 2018. Multi-hop teleportation in a quantum network based on mesh topology. Frontiers of Physics, 13(5), p.130314.

[15] Chakraborty, M., Mukherjee, A., Krikidis, I., Nag, A. and Chandra, S., 2025. A Hybrid Noise Approach to Modeling of Free-Space Satellite Quantum Communication Channel for Continuous-Variable QKD. IEEE Transactions on Green Communications and Networking, 9(3), pp.1311-1325.

[16] Ye, Z., Qian, X. and Pan, W., 2023. Quantum topology optimization via quantum annealing. IEEE Transactions on Quantum Engineering, 4, pp.1-15.

[17] Weinbrenner, L.T., Prasannan, N., Hansenne, K., Denker, S., Sperling, J., Brecht, B., Silberhorn, C. and Gühne, O., 2024. Certifying the topology of quantum networks: theory and experiment. Physical Review Letters, 132(24), p.240802.

[18] Li, Q., Wang, Y., Mao, H., Yao, J. and Han, Q., 2020. Mathematical model and topology evaluation of quantum key distribution network. Optics Express, 28(7), pp.9419-9434.

[19] Cacciapuoti, A.S., Caleffi, M., Tafuri, F., Cataliotti, F.S., Gherardini,

S. and Bianchi, G., 2019. Quantum internet: Networking challenges in distributed quantum computing. IEEE Network, 34(1), pp.137-143.

[20] Yu, N., Lai, C.Y. and Zhou, L., 2021. Protocols for packet quantum network intercommunication. IEEE Transactions on Quantum Engineering, 2, pp.1-9.

[21] Singh, A., Dev, K., Siljak, H., Joshi, H.D. and Magarini, M., 2021. Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions. IEEE Communications Surveys & Tutorials, 23(4), pp.2218-2247.

[22] Yu, R., Dutta, R. and Liu, J., 2022. On topology design for the quantum internet. IEEE Network, 36(5), pp.64-70.

[23] Hermans, S.L.N., Pompili, M., Beukers, H.K.C., Baier, S., Borregaard, J. and Hanson, R., 2022. Qubit teleportation between non-neighbouring nodes in a quantum network. Nature, 605(7911), pp.663-668.

[24] Xiao, Z., Li, J., Xue, K., Li, Z., Yu, N., Sun, Q. and Lu, J., 2023. A connectionless entanglement distribution protocol design in quantum networks. IEEE Network, 38(1), pp.131-139.

[25] Azuma, K., Economou, S.E., Elkouss, D., Hilaire, P., Jiang, L., Lo, H.K. and Tzitrin, I., 2023. Quantum repeaters: From quantum networks to the quantum internet. Reviews of Modern Physics, 95(4), p.045006.

[26] Huang, Y., Qi, Z., Yang, Y., Zhang, Y., Li, Y., Zheng, Y. and Chen, X., 2025. A sixteen-user time-bin entangled quantum communication network with fully connected topology. Laser & Photonics Reviews, 19(1), p.2301026.

[27] Begimbayeva, Y., Ussatova, O., Zhaxalykov, T., Akhtanov, A., Pashkevich, R. and Arshidinova, M., 2024. Development of superposition based quantum key distributin protocol in decentralized full mesh networks. Eastern-European Journal of Enterprise Technologies, 132(9).

[28] Cacciapuoti, A.S., Illiano, J. and Caleffi, M., 2023. Quantum internet addressing. IEEE Network, 38(1), pp.104-111.

[29] Jiang, J.L., Luo, M.X. and Ma, S.Y., 2024. Quantum network capacity of entangled quantum internet. IEEE Journal on Selected Areas in Communications, 42(7), pp.1900-1918.

[30] Pan, D., Long, G.L., Yin, L., Sheng, Y.B., Ruan, D., Ng, S.X., Lu, J. and Hanzo, L., 2024. The evolution of quantum secure direct communication: On the road to the qinternet. IEEE Communications Surveys Tutorials, 26(3), pp.1898-1949.

[31] Chandra, D., Babar, Z., Nguyen, H.V., Alanis, D., Botsinis, P., Ng, S.X. and Hanzo, L., 2017. Quantum topological error correction codes: The classical-to-quantum isomorphism perspective. IEEE Access, 6, pp.13729-13757.

[32] Song, S. and Hayashi, M., 2019. Secure quantum network code without classical communication. IEEE Transactions on Information Theory, 66(2), pp.1178-1192.

[33] Joshi, S.K., Aktas, D., Wengerowsky, S., Lončarić, M., Neumann, S.P., Liu, B., Scheidl, T., Lorenzo, G.C., Samec, Ž., Kling, L. and Qiu, A., 2020. A trusted node–free eight-user metropolitan quantum communication network. Science advances, 6(36), p.eaba0959.

[34] Bullock, M.S., Gagatsos, C.N., Guha, S. and Bash, B.A., 2020. Fundamental limits of quantum-secure covert communication over bosonic channels. IEEE Journal on Selected Areas in Communications, 38(3), pp.471-482.

[35] Cacciapuoti, A.S., Caleffi, M., Van Meter, R. and Hanzo, L., 2020. When entanglement meets classical communications: Quantum teleportation for the quantum internet. IEEE Transactions on Communications, 68(6), pp.3808-3833.

[36] Chen, Y.A., Zhang, Q., Chen, T.Y., Cai, W.Q., Liao, S.K., Zhang, J., Chen, K., Yin, J., Ren, J.G., Chen, Z. and Han, S.L., 2021. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature, 589(7841), pp.214-219.

[37] Pant, M., Krovi, H., Towsley, D., Tassiulas, L., Jiang, L., Basu, P., Englund, D. and Guha, S., 2019. Routing entanglement in the quantum internet. npj Quantum Information, 5(1), p.25.

[38] Hahn, F., Pappa, A. and Eisert, J., 2019. Quantum network routing and local complementation. npj Quantum Information, 5(1), p.76.

[39] Singh, A., Dev, K., Siljak, H., Joshi, H.D. and Magarini, M., 2021. Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions. IEEE Communications Surveys & Tutorials, 23(4), pp.2218-2247.

[40] Gaidash, A., Miroshnichenko, G. and Kozubov, A., 2022. Quantum network security dependent on the connection density between trusted nodes. Journal of Optical Communications and Networking, 14(11), pp.934-943.

[41] Cozzolino, D., Da Lio, B., Bacco, D. and Oxenløwe, L.K., 2019. High-dimensional quantum communication: benefits, progress, and future challenges. Advanced Quantum Technologies, 2(12), p.1900038.

[42] Gyongyosi, L. and Imre, S., 2018. Topology adaption for the quantum internet. Quantum Information Processing, 17(11), p.295.

[43] Li, C., Li, T., Liu, Y.X. and Cappellaro, P., 2021. Effective routing design for remote entanglement generation on quantum networks. npj Quantum Information, 7(1), p.10.

[44] Zhuang, Q. and Zhang, B., 2021. Quantum communication capacity transition of complex quantum networks. Physical Review A, 104(2), p.022608.

[45] Li, J., Jia, Q., Xue, K., Wei, D.S. and Yu, N., 2022. A connection-oriented entanglement distribution design in quantum networks. IEEE Transactions on Quantum Engineering, 3, pp.1-13.

[46] Granelli, F., Bassoli, R., Nötzel, J., Fitzek, F.H., Boche, H. and da Fonseca, N.L., 2022. A novel architecture for future classical-quantum communication networks. Wireless Communications and Mobile Computing, 2022(1), p.3770994.

[47] Li, J., Wang, M., Xue, K., Li, R., Yu, N., Sun, Q. and Lu, J., 2022. Fidelity-guaranteed entanglement routing in quantum networks. IEEE Transactions on Communications, 70(10), pp.6748-6763.

[48] Illiano, J., Caleffi, M., Manzalini, A. and Cacciapuoti, A.S., 2022. Quantum internet protocol stack: A comprehensive survey. Computer Networks, 213, p.109092.

[49] Wang, S., Yin, Z.Q., He, D.Y., Chen, W., Wang, R.Q., Ye, P., Zhou, Y., Fan-Yuan, G.J., Wang, F.X., Chen, W. and Zhu, Y.G., 2022. Twin-field quantum key distribution over 830-km fibre. Nature photonics, 16(2), pp.154-161.

[50] Grünenfelder, F., Boaron, A., Resta, G.V., Perrenoud, M., Rusca, D., Barreiro, C., Houlmann, R., Sax, R., Stasi, L., El-Khoury, S. and Hänggi, E., 2023. Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. Nature Photonics, 17(5), pp.422-426.

[51] Shen, S., Yuan, C., Zhang, Z., Yu, H., Zhang, R., Yang, C., Li, H., Wang, Z., Wang, Y., Deng, G. and Song, H., 2023. Hertz-rate metropolitan quantum teleportation. Light: Science & Applications, 12(1), p.115.

[52] Chawla, P., Ajith, A. and Chandrashekar, C.M., 2023. Quantum walk-based protocol for secure communication between any two directly connected nodes on a network. Physica Scripta, 98(10), p.105113.

[53] Zhang, Y., Li, H., Ding, T., Huang, Y., Liang, L., Sun, X., Tang, Y., Wang, J., Liu, S., Zheng, Y. and Chen, X., 2023. Scalable, fiber-compatible lithium-niobate-on-insulator micro-waveguides for efficient nonlinear photonics. Optica, 10(6), pp.688-693.

[54] Shi, S., Wang, Y., Tian, L., Li, W., Wu, Y., Wang, Q., Zheng, Y. and Peng, K., 2023. Continuous variable quantum teleportation network. Laser Photonics Reviews, 17(2), p.2200508.

[55] Howe, C., Aziz, M. and Anwar, A., 2024. Towards scalable quantum networks. arXiv preprint arXiv:2409.08416.

[56] Santagiustina, F.B., Agnesi, C., Alarcón, A., Cabello, A., Xavier, G.B., Villoresi, P. and Vallone, G., 2024. Experimental post-selection loophole-free time-bin and energy-time nonlocality with integrated photonics. Optica, 11(4), pp.498-511.

[57] Yang, Y., Li, Y., Li, H., Wu, C., Zheng, Y. and Chen, X., 2025. A 300-km fully-connected quantum secure direct communication network. Science Bulletin, 70(9), pp.1445-1451.

[58] Jaiswal, A., Kumar, S., Kaiwartya, O., Kashyap, P.K., Kanjo, E., Kumar, N. and Song, H., 2021. Quantum learning-enabled green communication for next-generation wireless systems. IEEE Transactions on Green Communications and Networking, 5(3), pp.1015-1028.

[59] Saad, H.M., Chakrabortty, R.K., Elsayed, S. and Ryan, M.J., 2021. Quantum-inspired genetic algorithm for resource-constrained project-scheduling. IEEE Access, 9, pp.38488-38502.

[60] Xu, Z., Shang, W., Kim, S., Bobbitt, A., Lee, E. and Luo, T., 2024. Quantum-inspired genetic algorithm for designing planar multilayer photonic structure. NPJ Computational Materials, 10(1), p.257.

[61] Magesh, G., 2024. Quantum Channel Optimization: Integrating Quantum-Inspired Machine Learning With Genetic Adaptive Strategies. IEEE Access, 12, pp.80397-80417.

[62] Narayanan, A. and Moore, M., 1996, May. Quantum-inspired genetic algorithms. In Proceedings of IEEE international conference on evolutionary computation (pp. 61-66). IEEE.

[63] Lin, D.Y. and Waller, S., 2009. A quantum-inspired genetic algorithm for dynamic continuous network design problem. Transportation Letters, 1(1), pp.81-93.