Optics Communications 596 (2025) 132549

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Optimizing qubit transfer in multi-host quantum network using security-oriented entanglement routing algorithm

Saumya Priyadarshini [a,*], Chandrashekar Jatoth [a], Rajesh Doriya [a], Rajkumar Buyya [b]

[a] Department of Information Technology, National Institute of Technology Raipur, G.E. Road, Raipur, 492010, Chhattisgarh, India
[b] School of Computing and Information Systems, The University of Melbourne, Parkville Campus, Melbourne, VIC 3010, Australia

ARTICLE INFO

Keywords:
Quantum protocols
Quantum simulator
OSI network protocols
Security entangled protocol
Qubits transmission

ABSTRACT

Quantum communication networks exploit qubit superposition and entanglement to achieve high-efficiency, provably secure data exchange via QKD and quantum-safe cryptography, with recent architectures reducing channel vulnerabilities for scalable, tamper resistant transmission. To address these challenges, this work proposes SO-ERA$_{Sim}$ (Security-Oriented Entanglement Routing Approach Simulator), an OSI-layered quantum network simulator from the physical to application layer. SO-ERA$_{Sim}$ integrates classical–quantum hybrid computing to transmit qubits via quantum networking protocols, incorporating a security-oriented entanglement protocol to enhance data transmission security in quantum networks. Leveraging entanglement swapping, SO-ERA$_{Sim}$ minimizes overhead by selecting high-fidelity paths via intermediate nodes, optimizing entangled-pair utilization, memory allocation, and communication cost, while preserving fidelity in multi-host networks through quantum error correction, purification, multiplexing, and efficient classical channel coordination. Quantum key generation is synchronized through qubit-based timing, employing adaptable latency mechanisms with dynamic key renewal and latency-tolerant protocols. However, real-time error correction in teleportation and superdense coding remains constrained by substantial memory demands for continuous quantum state monitoring. The cross-layer attack simulation model extension targeting entangled states during swapping operates on time-lag dependencies across all OSI layers and evaluates hybrid networks for simulation integrity which validates the effectiveness of SO-ERA$_{Sim}$ in secure quantum communications.

1. Introduction

Quantum communication uses the fundamental principles of quantum mechanics to facilitate the transfer of information. Information is transmitted in the form of qubits [1]. This makes it feasible to develop unique potential that are impossible to achieve through the classical communication methods [2]. The latest advances in it include quantum communication networks [3]. Establishing an encryption key between end to end nodes in a network can be done securely through QKD [4,5], a well-known use of quantum communication. The primary objective in quantum communication is the transmission of photonic [6], entanglement across large distances among the nodes involved. This technique creates a quantum channel that preserves the inherent quantum correlations of entangled particles. These include quantum teleportation, which transmits an unknown quantum state without the particle being physically transmitted. To encode quantum information in qubits for teleportation, photon polarization [7], is employed. QKD securely exchanges cryptographic keys based on quantum principles, quantum secret sharing enables the safe distribution of private information among multiple parties and dense coding enhances the transfer of information by entangling multiple bits of classical data into a single qubit. The development of secure and adaptable quantum communication framework [8], depends on the ability to disperse entanglement over large networks.

Utilizing a conventional method to establish a connection with quantum devices [9], suggests that there is an immediate requirement to speed up the assessment and development of quantum communication protocols [10], and applications [11]. To meet this goal, we need to make progress in a number of areas, including hardware network architectures. It is even more important to make simulation tools for quantum networks to understand and model how these systems interact with each other [12]. The primary phase of tool address significant issues in quantum network research by providing a flexible simulation environment. It facilitates real-time lab connections and ensures uninterrupted interaction between experimental environments. [13, 14].

* Corresponding author.
E-mail addresses: spriyadarshini.nit@gmail.com (S. Priyadarshini), chandrashekar.jatoth@gmail.com (C. Jatoth), rajeshdoriya.it@nitrr.ac.in (R. Doriya), rbuyya@unimelb.edu.au (R. Buyya).

https://doi.org/10.1016/j.optcom.2025.132549
Received 18 June 2025; Received in revised form 8 August 2025; Accepted 9 October 2025
Available online 17 October 2025

The primary goal of SO-ERA$_{Sim}$ is to provide a comprehensive framework that allows users to develop quantum networking simulators using communication protocols easily. With this framework, users will not have to depend on software-specific activities such as managing threading and synchronization. To accomplish these goals, SO-ERA$_{Sim}$ enables the creation of quantum network protocols as described in the paper. The objective is to facilitate users' rapidly generating protocols for the efficient and secure [15], transport of qubits within quantum systems. SO-ERA$_{Sim}$ simplifies noise modeling by taking into account perfect sync with constant time-independent errors in both quantum and classical systems. Timing delays and complex interference patterns can affect real-world performance. It models decoherence via Markovian noise channels characterized by consistent error rates and ideal synchronization, facilitating scale simulation. To show OSI layer interdependencies and synchronize event processing through layered control, the simulator combines quantum and classical communication protocols in a hybrid architecture. To compensate for latency and error propagation between layers, quantum events, such as entanglement generation, are synchronized with classical communication, such as control messages, via a time-synchronized event queue.

It is limited by inadequate noise models, static attack scenarios, and the absence of integrated cross-layer quantum classical threat simulations. The proposed trade-offs between security and scalability require hardware validated enhancements. The framework uses the entanglement based routing technique [16], which assumes that pairs of hosts are directly entangled. However, with thousands of simultaneous entangled state transfers, physical qubit and channel restrictions might cause failures or delays. SO-ERA$_{Sim}$ authenticates the realism and physical viability of its protocols using empirically validated noise models [17], benchmarking, Monte Carlo simulations, verification procedures, and cross-validation with alternative simulators. These methodologies guarantee precise and viable simulations across various hardware environments while considering hardware-specific limitations, guaranteeing reliable performance across many contexts despite the lack of physical quantum hardware.

In the area of quantum networks, there is a strong correlation between the structure of communication protocols described in research papers and the methodologies applied when developing simulations with the SO-ERA$_{Sim}$ simulator. In future, we intend to make the SO-ERA$_{Sim}$ simulator more precise.

The primary contribution of this study is summarized as follows:

1. A novel hybrid communication framework in the SO-ERA$_{Sim}$ simulator, integrating classical and quantum channels to enable secure qubit transmission. Our framework employs a quantum key distribution (QKD) based protocol, achieving enhanced security and efficiency compared to traditional quantum communication methods.
2. The security-oriented entangled protocol leverages quantum entanglement across the physical, network, and application layers. This protocol ensures robust end-to-end security in quantum networks, outperforming existing protocols limited to single-layer security.
3. To evaluate the SO-ERA$_{Sim}$ simulator's performance in a multi-host quantum network by measuring latency, throughput, and error rate. Our results demonstrate superior scalability and reliability compared to state-of-the-art simulators, validating the simulator's effectiveness for large-scale quantum network simulations.

This article will describe the SO-ERA$_{Sim}$ simulator, including its architecture, implementation, and operation principles.

The rest of the paper is structured as follows. Section 2 describes related work, framework is described in Section 3. In Section 4, we have presented the design of our proposed framework. Section 5 describes the implementation of the proposed method. Section 6 introduces the computational backend technology. Sections 7 and 8, describes methodological approach and performance evaluation. Section 9 concludes with summary of results.

2. Related work

Conducting a comprehensive literature study, we found many significant issues in quantum network modeling. These include scalability, accurate simulation of entanglement, efficient error correction, and integration with conventional networks. Our platform provides tailored functionalities to address these difficulties efficiently.

Recent implementations like $SeQUeNCe$ simulate a nine-router photonic quantum network. Table 1, compares SO-ERA$_{Sim}$ to other quantum networking simulation tools to see how it stacks up against the competition and what makes it distinct. This simulator includes hardware, entanglement, network, application, and resource components. These modules simulate numerous quantum network components, aiding quantum communication protocol research [25]. To execute quantum circuits, the author suggested a $Qiskit$ [21], simulator and demonstrated attack that use it in conjunction with the superdense Quantum protocol. Moreover, It provides additional insights by showing the Quantum Recursive Network Architecture (QRNA) [26], which employs Rule Set-based connections through a two-pass setup. Building on the work of enabling global communication, QKD has progressed from laboratory proofs to a secure, large-scale space-to-ground network [26,27]. This is further supported by $NetSquid$ [20], a discrete-event simulator for quantum networks and modular quantum computing system, from physical to application layers. The possibilities of $NetSquid$ are demonstrated by repeater chains, quantum switch control planes, and networks consisting of one thousand nodes [28]. In contrast to NetSquid, SO-ERA$_{Sim}$ optimizes protocols like entanglement, teleportation, avoiding detailed analysis of physical layer noise, latency and hardware specific restrictions. SO-ERA$_{Sim}$ is protocol-efficient, while NetSquid is hardware-accurate. It illustrates protocol correctness through validated quantum operations, scalability through abstracted noise models, and hardware independence by rejecting platform-specific characteristics.

SO-ERA$_{Sim}$ integrates performance, quality, and hardware uncertainty with a modular architecture, enhanced noise designs, tensor network techniques, high-performance computing integration, and strict benchmarking. These criteria guarantee effective, realistic simulations across many devices, addressing trade-offs to uphold high authenticity.

A similar perspective is shared by $QuNetSim$ [19], a framework that accurately models quantum networks at the network layer through a user-friendly interface. Users can easily develop and create link layer protocols to explore and test quantum networking protocols in different situations. $QuNetSim$ offers the ability to easily customize current quantum network protocols for specialized research and testing purposes [29]. Simulation findings show that distribution rates are preserved while entanglement fidelity is improved by increasing router multiplexing depth [30]. SO-ERA$_{Sim}$ protocol design eliminates the flaws of QuNetSim and SeQUeNCe through the use of robust noise models, adaptive purification protocols, fidelity-conscious routing, and optimized simulation methodologies. These characteristics improve entanglement fidelity and decrease error rates in extensive quantum network simulations, guaranteeing more realistic and resilient performance.

An extension of this idea can be found in [31], the SQDSQC uses single photons in polarization and spatial-mode degrees of freedom for eavesdropping checks and message encoding using two unitary operations. A comprehensive security assessment [32] has verified that it is highly resistant to a range of well-known attacks, such as impersonation, interception and resend, and impersonated fraudulent assaults. In [18], Quantum key communication protocol is created using N-bit keys, optical multiplexers, demultiplexers, and quantum repeaters using entanglement switching. This is further supported by the research of $QuISP$ [18], simulation which validates enormous quantum network against smaller network analytic results under feasible, noisy, and heterogeneous environments. It simulates and develops complicated quantum internet protocols on a laptop with thousands of qubits and hundreds of nodes [33]. However, it offers a different

Table 1
Technical comparison of SO-ERA$_{Sim}$ with other related works based on protocols, network Layers, and communication Channels.

Sr. No.	Simulator/ Framework	Protocols	Methods	Quantum	Classical	Communication Layers
1	Qinternet [1]	Point-to-point	QSDC (Quantum Secure Direct Communication)	✗	✓	Network
2	QuISP [18]	Entanglement Generation, Swapping, Purification	Event-Driven Simulation with OMNeT++	✗	✓	Network
3	QuNetSim [19]	QKD, Teleportation	Routing with Entanglement	✗	✓	Network
4	NetSquid [20]	Control Plane Protocols	Singular-Event Modeling, Layer-by-Layer Modeling	✓	✓	Physical
5	IBM Quantum [21]	Quantum Superdense Coding	Quantum Superdense	✓	✓	Network
6	SeQUeNCe [22]	Entanglement Management	Singular-Event Modeling	✓	✓	Application
7	QKDSim [23]	B92, QKD	Development of a Simulation Toolkit	✓	✓	Network
8	SimulaQron [24]	Quantum Teleportation, Entanglement Creation (EPR)	BB84 State Preparation and Transmission	✓	✓	Link and Physical Layer
9	SO-ERA$_{Sim}$ (Proposed)	Hybrid and SO-ERA	Quantum and Classical Programming	✓	✓	Physical to Application layer

viewpoint, suggesting using the Bell test to identify entanglement and create an exchange of data between sender and receiver for robust quantum communication. This ensures simplicity, simple integration into current frameworks, and resilience to defective equipment [34]. Zhang et al. [35], discussed that implementing quantum technology in existing infrastructure improves efficiency and safety for future communication systems. It covers basic concepts, design goals, protocols, prospective applications, and problems.

The author in [36] analyzed a new quantum authentication system that uses individual photons based on quantum private direct interaction to authenticate the user's identity without revealing the pre-shared encryption key. Quantum technology and communication, including polarization and quantum connectivity, and their roles. It also encompasses quantum communication systems, optical fiber cable teleportation, quantum encryption, satellite communication, and quantum memory [19]. In [20], the author examines how multipath routing strategies optimize quantum communication networks. These protocols carry quantum signals across numerous routes to minimize delays and increase throughput, improving performance and intrusion security. Chen et al. [37], analyzed a DI-QSDC protocol, which uses very efficient single-photon sources to secure communication by observing Bell-inequality violations. Two sequential integer programming issues are used to suggest efficient routing algorithms [38], and analyze their time complexity and performance constraints.

SO-ERA$_{Sim}$ inherently incorporates key quantum network traits including key rate through QKD protocol, distance by multi-hop routing, and efficiency by qubit transmission, while emphasizing scalability through noise abstraction. It includes a wide variety of benchmarking criteria including fidelity, scalability, hardware flexibility, resource efficiency, software flexibility, reproducibility, and circuit depth capabilities, in addition to latency, throughput, and error rate. The network methodologies, realistic noise models, high-speed computing integration, and modular architecture provide precise, scalable, and flexible simulations.

SO-ERA$_{Sim}$ ensures fidelity to real-world limitations by employing accurate noise models, Monte Carlo event simulation, dynamic protocol optimization, hardware-agnostic design, and security validation methods. These capabilities provide precise simulation of quantum memory limits, repeater functionalities, and the maintenance of long-distance entanglement, while guaranteeing that security assumptions conform to physical limitations for protocols such as QKD.

3. SO-ERA$_{Sim}$ framework

The primary goal of our proposed SO-ERA$_{Sim}$ is to simulate quantum communication networks. We strive to provide a platform that enables the testing and validating of robust protocols designed explicitly for quantum communication networks. Users can create network configurations using SO-ERA$_{Sim}$ that utilize both conventional and quantum communication between nodes. It optimizes concurrency by distinguishing between classical and quantum channels, utilizing event-driven scheduling and global clocks for syncing. It combines low-latency classical input with quantum operations, facilitates real-time protocols such as QKD, teleportation. It utilizes parallel processing with correction of errors to guarantee scalable, secure administration of quantum states. The user can define the behavior of each node. It improves the complex process of overseeing multiple processes by providing techniques for connecting nodes within a large network [39]. During transmission across quantum channels, coherence preservation at the physical layer maintains qubit superposition, entanglement, quantum error correction, privacy amplification, and fidelity.

In addition, SO-ERA$_{Sim}$ includes a wide variety of security-oriented protocols, including teleportation [31], entanglement [40], superdense coding [41], hybrid protocols etc. By using fundamental protocols as the base parts, these quantum communication protocols are specifically designed to function on arbitrary quantum networks. It provides a mechanism that is effective and efficient for constructing complex networks, enabling users to build and evaluate security. To organize their operations, SO-ERA$_{Sim}$ simulators frequently take the Open Systems Interconnection (OSI) paradigm as their source of inspiration. It manages interlayer dependencies via implied parameters transmission like Qubit objects inheriting host configurations and synchronous protocol chaining, such as QKD directly facilitating message encryption. However, in addition to this, they also contain unique quantum protocols and procedures [21]. The management of classical and quantum data is a common challenge for simulators. Accurate OSI model stacking cannot be employed in subsequent quantum network implementation [42], and additional levels can be developed. Simulators often use a mixture of traditional communication methods to provide safe connections between the hosts. The fundamental principle of layering, which is present in classical communication networks, is expected to be applied in quantum networks. These levels will be application, transport, network and physical layers. Quantum information, known as qubits, will be encrypted and then converted into data packets. These data packets will be transmitted over a network to ensure that they reach their

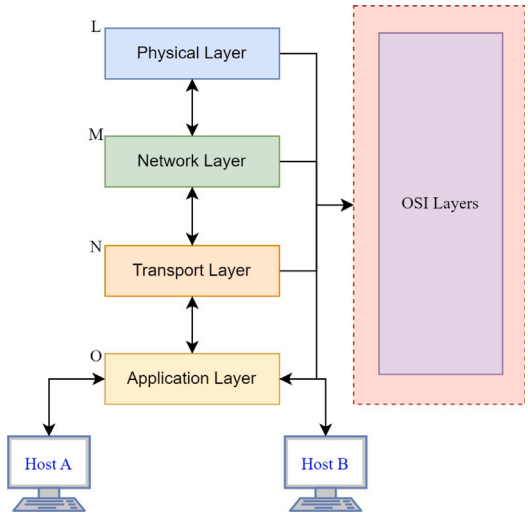

Fig. 1. Utilization flow of OSI layers in quantum communication.

intended destination. Enables hybrid architectural solutions to quantum network OSI layering constraints. It allows real-time fidelity tracking across layers by directly linking physical-layer qubit operation to network-layer routing decisions. Protocol authenticity overcomes architectural purity for entanglement dependent procedures where layer separation fails. The confidentiality of the information will be maintained through this procedure.

We illustrate the architectural framework of SO-ERA$_{Sim}$ in Fig. 1 which include four network layers, specifically designated as L, M, N and O with different tasks. To ensure the reliable and secure transmission of qubits. In this particular scenario, a "virtual connection" refers to the link between host A and host B, even though the data transmitted from host A is relayed through multiple intermediate nodes in the network with security. The Fig. 1 illustrates the connection between nodes through classical channel depicted by dotted lines and a quantum channel depicted by thick lines. Both forms of communication are processed using a system that involves layering, which enables the network to direct both types of information based on the content of the packets. Users can utilize the same logic to send both classical and quantum data, with the lower layers responsible for managing any discrepancies. SO-ERA$_{Sim}$ emphasizes the physical layer in its implementation, as this layer is responsible for the production, coding, and transmission of qubits across quantum channels, such as optical fibers or free-space optics. The physical layer automatically ensures security by leveraging the basic characteristics of quantum physics [3]. Key security features include identifying eavesdropping, preventing cloning, and utilizing entanglement for secure communications [43].

Hence, the physical layer that exists in our concept is of utmost importance in guaranteeing the security and secrecy of the transmitted data. The network layer can efficiently route and transmit quantum information throughout the network [44]. The simulation of the transport link in SO-ERA$_{Sim}$ is straightforward, requiring a dependable connection between two nodes. However, the larger simulation of the network is encompassed by SO-ERA$_{Sim}$. While it is reasonably easy to simulate the behavior of the network layer in SO-ERA$_{Sim}$, the modeling of the physical layer is included within the scope of SO-ERA$_{Sim}$.

When it comes to achieve secure communication between hosts, SO-ERA$_{Sim}$ simulator evaluates the impact of noise and decoherence utilizing comprehensive physical-layer models and fidelity metrics, while mitigating these affects through quantum error correction, entanglement purification, noise-aware routing, and dynamical decoupling. This guarantees consistent routing accuracy and protocol integrity across various multi-host topologies, balancing simulation with computational performance.

4. DESIGN

OF SO-ERA$_{Sim}$

SO-ERA$_{Sim}$ aims to facilitate the creation of simulations that provide sufficient accuracy to enable the development, testing, and debugging of applications for quantum communication networks [45], while ensuring security for a proof of concept phase. To facilitate application development by a wide range of users, we maintain a high degree of security and efficiency. SO-ERA$_{Sim}$ enables users to combine many security-oriented protocols, which may be readily customized and simulated to operate in parallel or sequential setups.

The overall network architecture of the SO-ERA$_{Sim}$ simulator is depicted in Fig. 2 for a quantum communication system, enabling safe data transfer inside a multi-host topology comprising hosts L, O, M, and N. The physical layer divided into an encoding layer at Host L and a decoding layer at Host O, is responsible for processing raw data into quantum states. Decoding occurs thereafter, with the physical layer encoding block managing encoding according to the channel and minimizing noise. The security layer at Host O defines processes as QKD, whereas the implement security layer achieves these protocols, protecting data integrity and confidentiality by integrating security measures into the quantum states. The End-to-End Layer, involving Host M (sender) and Host N (receiver), regulates the whole communication route, hiding inherent complications. Data transmits from encoding at Host L through the physical layer encoding to decoding and security implementation at Host O, resulting in end-to-end delivery, with feedback loops for dynamic modifications based on performance measurements. This architecture reduces quantum noise and decoherence by integrated error correction, facilitates distributed routing throughout the topology, and guarantees strong security, making it appropriate for specialized quantum network applications.

Each host participating in the transmission process plays a vital role in guaranteeing the secure transfer of qubits. The layers represent several stages of communication, starting from the initial configuration, encoding, and ending with the final reception and decoding, while also incorporating security mechanisms to protect the data. This systematic approach guarantees the accurate transfer of encoded data within the qubits, together with strong security mechanisms, thus providing both precision and confidentiality across the network. It ensures a consistency in qubit state transitions using a centralized state management system employing time stamped activities, thus ensuring causal ordering between intermediary hosts. It coordinates quantum computations with classical control signals, so preventing conflicts and maintaining the integrity of the qubit chain throughout multi-host interactions, noise-aware simulation, state monitoring with fidelity metrics, QEC, high-precision synchronization, and SWAP-optimized routing.

To maintain entanglement fidelity among distant nodes in multi-hop entanglement transfer, a number of particular steps must be taken in order to detect, log, and correct quantum state problems during transmission. In multi-hop entanglement transfer, mid-route quantum state problems are detected by means of syndrome measurements with stabilizer codes while problems are simultaneously recorded using a distributed event system. Correction makes use of entanglement purification and quantum error correction codes (such as surface codes), employing real-time feedback to start corrective actions that maintain fidelity.

In network, qubits are transferred between hosts through the use of hybrid protocols and entanglement techniques that prioritize security. The hybrid protocol integrates both quantum and conventional interaction between hosts. The system utilizes QKD to generate a secure key and subsequently applies symmetric encryption to it for secure classical communication. This strategy enhances the security, utility, and efficiency of information transfer. Incorporating a security-oriented entanglement approach enhances the security of data transmission in quantum networks by leveraging entangled qubits. This technology utilizes the distinct characteristics of quantum physics to establish a

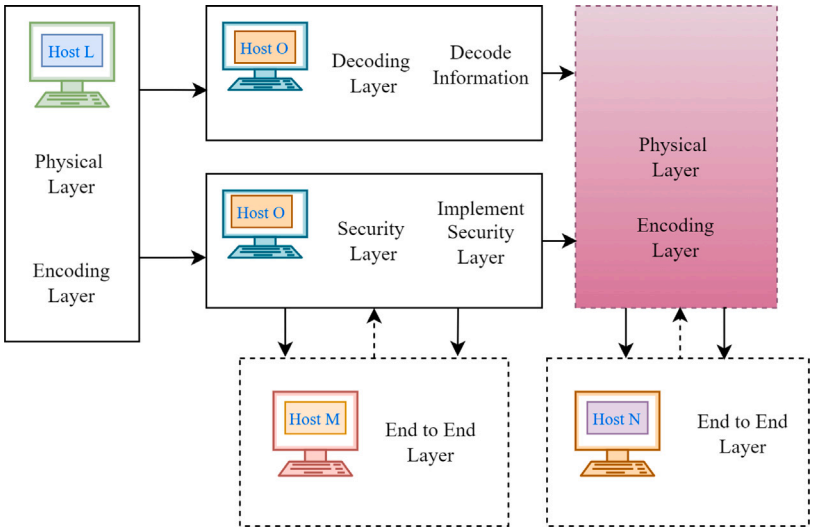

Fig. 2. SO-ERA$_{Sim}$: Enabling realistic simulations for quantum communication network.

quantum network that enables secure and efficient communication between network nodes using a security-oriented entanglement-based routing algorithm. An illustration of this process may be found in Section 4. SO-ERA$_{Sim}$ contrasts between quantum and conventional memory by allocating distinct data structures, quantum memory remains qubit states with coherence monitoring, while classical memory manages control data, measurement outcomes, and routing information. Each functions under certain access regulations and periodic limitations to ensure a clear distinction during transit and decoding.

Finally, the receiver will read the qubit's header to figure out what to do with the qubit when it has completed traversing over the network and reached the receiver host. It follows that the qubit is stored either in conventional memory or one of the two quantum memories developed for use in quantum computing. With the help of these two quantum memories, users may differentiate between qubits provided directly by the sender and qubits created via security-oriented entanglement techniques. SO-ERA$_{Sim}$ models key management attacks, including key theft during quantum key distribution (QKD), decoding risks by eavesdropping with error rate analysis, and encoding uncertainties like illegal state manipulation and noise injection. To assess vulnerabilities, it uses event-driven simulations that include dynamic key refresh and entanglement purification, enabling flexible countermeasures across multi-host topologies. In order to support dynamic topologies characterized by intermittent connection failures and node reassignments. The architecture will employ real time topology discovery and adaptive routing to revise pathways. It would facilitate multi path entanglement distribution and decentralized node coordination for rerouting and function transfer incorporating real time error correction to address instability.

To summarize, the SO-ERA$_{Sim}$ employs distinct layers that resemble the OSI framework. It includes hybrid protocols and security-oriented entanglement techniques that prioritize security and numerous tasks simultaneously without disrupting the primary application, enabling more effective operations. A strategic use of QKD [46], to create a secure key and then applies symmetric encryption to ensure safe classical communication [47]. This technique improves the security, functionality, and effectiveness of qubit transmission. By utilizing this technique, the security, usefulness, and efficiency of the information transmission process are improved. This technique handles the transmission of data, the receiving of acknowledgments, and the waiting for information from other hosts with security, efficiency and reliability.

5. Implementation of SO-ERA$_{Sim}$

This section outlines the key characteristics of SO-ERA$_{Sim}$ for implementing hybrid and security oriented entanglement routing protocols. Qubit is an essential data structure in SO-ERA$_{Sim}$ that linked to a particular host and give a unique identifier upon creation. Qubit is created by implementing the Qubit class using host. Once a host has created a qubit, it can undergo logical operations to store it or be transferred to another host. We use internal verification to identity qubit conflicts and duplication while running on various hosts. Globally unique identity formation using host specific IDs, timestamps, random seeds, synchronization protocols via message-passing interfaces (MPI), distributed hash-based conflict detection, and periodic validation during critical operations like entanglement distribution assure network uniqueness.

Several ways are available for transmitting a qubit, such as direct transmission, entanglement, teleportation, superdense coding, hybrid methods, and Security-Oriented Entanglement Routing based approach.

The processes employ Qubit techniques:

1. The `send_qubit` method facilitates the direct transmission of a qubit to another host and indicates that a qubit is being sent by printing a message.
2. The `qubit_to_teleport` method is used to initialize a qubit to teleport it to another host.

Certain protocols allow hosts in SO-ERA$_{Sim}$ to create entangled qubits with one another. This is achieved through the use of the following host methods:

1. `entanglement_protocol`
2. `Quantum_teleportation_protocol`
3. `superdense_protocol_method`
4. `Quantum_key_distribution`
5. `secure_entanglement_setup`

After initializing and connecting hosts, they are started sequentially. A host starts by initializing its state and prepares to transmit and receive qubits. Protocol for transmitting and receiving the qubits between hosts are simulated. The host class' `sender_protocol` method sends n qubits to a recipient host, while the `reception_protocol` method waits for and measures them.

To manage consistency in memory state it employs a global timestamp system to sequence both classical communications, such as routing metadata, and quantum messages, such as qubit state updates, so

maintaining correct ordering despite asynchronous arrivals. Furthermore, it dynamically implements error correction and entanglement purification to alleviate decoherence. Entanglement swapping mechanism is used to guarantee entanglement maintenance during host transfer and logical procedure. This protocol eliminates the necessity for unitary transformations to characterize Bell states, hence diminishing complexity and resource requirements It depends on logical entanglement distribution to preserve fidelity among nodes.

Programmable hosts can retrieve and await incoming classical or quantum messages. Classical and quantum messages are stored in separate memory structures at the host. Hosts can retrieve information stored in their memories for activities. Here are the methods:

1. `get_data_qubit`
2. `receive_qubit`
3. `measure`
4. `send_measurement_results`
5. `measure_rectilinear`
6. `measure_diagonal`
7. `communicate_basis`
8. `encrypt_message`
9. `decrypt_message`

The Host class contains a wait parameter that defines a timeout duration for waiting to get a qubit from the next host. The current timeout limit is set to 10 s, which determines the duration that the host will be waiting for a qubit before determining that it has not been received. If the specified timeout period is exceeded, the procedure will return. None, indicating that the qubit failed to appear within the designated time frame. Various techniques can be employed to establish and terminate connections to create a network of hosts. In SO-ERA$_{Sim}$, connections are one-way and can be exclusively classical, quantum, or a hybrid. The host approaches are outlined below:

1. `add_connection`
2. `add_connections`
3. `add_node`
4. `get_node`

The start() method is utilized to initialize a Host. After initiating the Host, it can execute customized protocols using the `run_protocol` method. The `run_protocol` method, within the context of the Host class and network functions, is specifically designed to execute distinct communication protocols between hosts. This method is commonly used to start and control the intricate series of activities required for protocols such as entanglement distribution, quantum teleportation, or superdense coding. The protocol function, target receiver host are supplied as arguments. The approach guarantees the accurate execution of the protocol stages, effectively coordinating the actions between the sending and receiving hosts. SOERAsimSO-ERA$_{Sim}$ is scalable to moderate-to-large node counts, accommodating approx 100 nodes in a multi-host environment, facilitated by its modular design and parallel event processing capabilities. Performance measures, including entanglement success rate, memory utilization, latency, key rate and simulation throughput, inform dynamic resource allocation. It facilitate the equilibrium of fidelity, timeliness, and computing efficiency as network sizes expand.

Within the framework of the Sender Protocol, such as in a quantum teleportation protocol, the `run_protocol` function can trigger the series of actions where the sender read qubits, entangles them, carries out measurements, and transmits the results to the receiver. The framework of the Receiver Protocol encompasses the reception of the measurement outcomes, execution of conditional operations, and finalization of the quantum state teleportation process. Constructing the network architecture is a crucial aspect of every simulation. SO-ERA$_{Sim}$ employs a network singleton object to encapsulate the traditional and quantum networks. After the network topology has been built between the hosts, the hosts are incorporated into the network using the network methods `add_host`. The network constructs a graph by utilizing the connections of the hosts, which is then employed for hybrid and security-oriented entanglement routing algorithms. Every quantum communication protocol incorporates a blend of quantum activities, such as entanglement and teleportation, along with classical message exchange, such as transmitting measurement outcomes and conveying encryption keys. It incorporates integration and unit testing to validate protocol fidelity over diverse noise profiles, especially depolarizing, and topology configuration including stress tests and Monte Carlo methods. The timing performance is assessed through real-time examination of latency and throughput, while regression testing and comparisons with analytical models ensure consistency and accuracy.

6. Backend technologies in quantum computing

The SO-ERA$_{Sim}$ utilizes a hybrid and security-oriented entanglement routing method that prioritizes security to simulate qubits in a quantum communication network. The prior research has utilized many backend qubit simulators each with distinct efficiency. The mentioned projects include $ProjectQ$, $EQSN$, and CQC.

Overview of Qubit Backend Simulators: ProjectQ is renowned for its exceptional runtime speed. However, prolonged protocol execution leads to decreased efficiency owing to the accumulation of numerous qubit entanglements, resulting in reduced resilience. In the field of quantum communication, the simulator $EQSN$ (Efficient Quantum Secure Network) is a tool used to properly examine the efficiency of quantum communication systems. This includes measures such as key generation rate, error rates, and the effect of interference and losses in quantum channels. It can be applied to maximize the allocation of entanglement and the positioning of quantum repeaters in a quantum network. One specialized feature is the ability to assess how secure quantum communication protocols are against different types of attack and eavesdropping. Putting emphasis on network situations incorporating quantum connection and state teleportation, it offers a framework for creating and evaluating quantum communication protocols.

To improve communication system performance and security, conventional and quantum channels for communication are integrated into a process known as classical-quantum communication (CQC). Hybrid system modeling and analysis can be done with CQC simulators, which emphasize the optimizations and interactions of the systems. SO-ERA$_{Sim}$ determines whether CQC simulates more accurately than a fully quantum backend based on specific criteria. Due to classical optimization, system size, noise levels, and protocol complexity, hybrid models outperform other models in mixed classical-quantum tasks. Accuracy is measured by comparing execution time, error rate, and fidelity to pure quantum back-ends. Following benchmark testing across topologies and noise profiles, hybrid models with comparable fidelity and lower resource requirements are selected. They are crucial for researching error correction, creating and testing protocols such as QKD, and assessing the impact of noise in real-world quantum networks. $QuNetSim$ and $NetSquid$ belong to the CQC type offers a framework for modeling quantum networks that contain both quantum and classical components.

$QuTiP$ is a free and open-source python package for quantum system simulation. It is extensively used in quantum mechanics, optics, and information research. $QuTiP$ interfaces with other Python functions and can simulate and interact with quantum systems, solve Hamiltonian dynamics, and solve Lindblad master equations. Its versatility and advanced functionality make it excellent for educational, quantum computing, and communication research. An abstraction layer standardizes noise parameters such as decoherence rates, gate error, noise models, QPU calibration, volumetric benchmarking, non-Markovian noise handling, and error mitigation probability to address backend technology noise modeling differences. Backend-specific noise models

Fig. 3. Transferring data qubits in a multihost network.

are translated into a common format for consistent benchmarking, adequate protocol comparison, and deviation reporting for analysis.

SO-ERA$_{Sim}$ dynamically selects backend simulators by integrating protocol requirements such as fidelity, execution time, and qubit count with capabilities like statevector, stabilizer through cost-function analysis to enhance performance across various topologies and noise profiles. It eliminates backend constraints by employing approximation methods for substantial entanglement depth, utilizing error models to replicate fidelity degradation, and delegating precision sensitive tasks to more accurate simulators. It incorporates validation layers to identify and rectify deviations, guaranteeing uniform protocol performance across various backend functionalities. SO-ERASim's backend simulator design and parameters must be modified to accommodate thousands of qubits. To manage complex entanglement in various applications, state vector-based backends would be replaced with more scalable matrix product state, tensor networks, and hybrid classical-quantum systems. This scale requires advanced error mitigation methods such as zero noise extrapolation and variational noise modeling.

7. Methodological approach

7.1. Quantum communication protocol

In this section, six distinct approaches have been examined. Four techniques have been determined, while two have been newly established through a comprehensive analysis of existing literature.

The established approaches include qubit exchange, entanglement, teleportation, and superdense coding. The newly developed methods combine hybrid protocols and a security oriented entanglement routing algorithm. Based on analysis of many research articles, the procedure for transferring qubits in quantum communication operates in the following manner. Initializes a qubit that is connected to a host and can be expressed as vectors in a two-dimensional Hilbert space as Eq. (1).

$$q = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

where q (qubit), α and β are complex values as:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

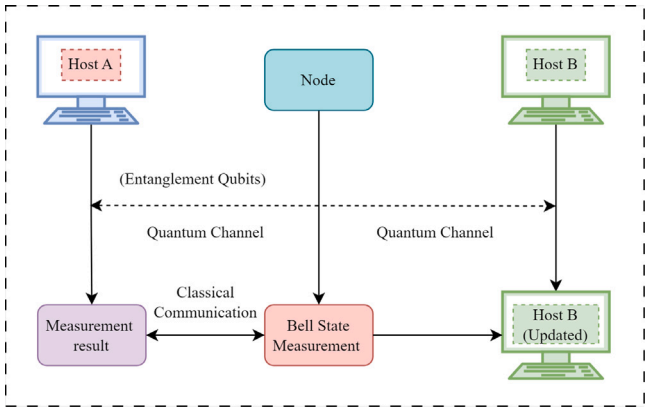

Fig. 4. Quantum entanglement process for secure quantum communication.

The qubit is placed in a superposition by applying the Hadamard gate H where H is given by Eq. (3).

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{3}$$

$$H(\alpha|0\rangle + \beta|1\rangle) = \frac{1}{\sqrt{2}}(\alpha(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}\beta(|0\rangle - |1\rangle)) \tag{4}$$

The transmitter host makes 6 qubits, performs the Hadamard gate to them, and transfers them to the receiver. The Hadamard procedure leaves each qubit in:

$$q_i = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{5}$$

When qubits arrive, the receiver measures them and records the outcomes. The measurement transforms the qubit's state to $|0\rangle$ or $|1\rangle$.

An initialized network consists of hosts X, Y, Z, L, M with their connections forming a graph shown in Fig. 3: $G = (V, E)$ where, V = (Vertices), E = (Edges). Host X Begin the process of setting up and preparing six qubits and apply the Hadamard gate to each qubit. Transmit each qubit to Host M. Perform a measurement on each qubit that is received and record the measurement outcomes as either 0 or 1.

Essentially, it emulates a quantum communication system in which qubits are generated, placed in superposition, transmitted between nodes, and measured, replicating the fundamental procedures of quantum protocols for communication. After the initial qubits are transmitted between parties or nodes, Quantum communication requires the establishment of an efficient method of communication. To do this, the idea of quantum entanglement is used as shown in Fig. 4, in which two qubits become connected state Even if they are physically apart. At the outset, X and Y, both qubits are initialized as state $|0\rangle$. By utilizing the Hadamard gate (H) on their individual qubits, they transform the state of each qubit from $|0\rangle$ to a superposition state:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{6}$$

The resultant state of both qubits after transition is as:

$$|\psi\rangle_{xy} = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \tag{7}$$

The resultant of the given qubit after hadmard operation by Eq. (7) of four quantum states, each with an equal probability amplitude of $\frac{1}{2}$.

X transmits q_x to Y, granting the ability to modify both qubits. Y performs a CNOT operation with q_y as the control and q_x as the target qubit. To activate the CNOT gate, the control qubit has to be in the state $|1\rangle$ before it can swap the target qubit's state.

$$\text{CNOT}_{xy} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \tag{8}$$

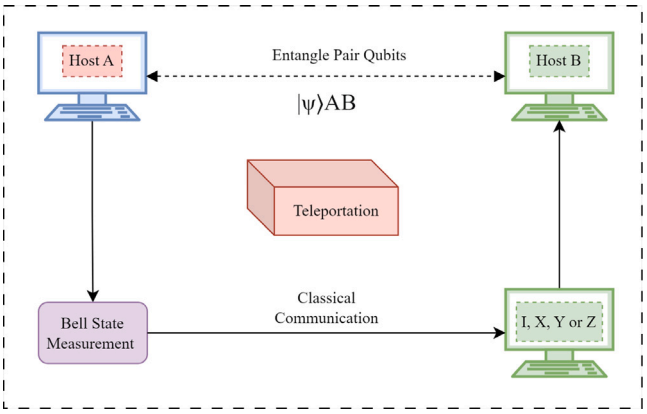

Fig. 5. Quantum teleportation process for secure quantum communication.

Upon measurement of q_x, q_y, the quantum state collapses into a specific state with a certain probability. The outcomes are as $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. Entanglement links these outcomes. If q_x measurement results in $|0\rangle$, q_y measurement will also result in either $|0\rangle$ or $|1\rangle$, and conversely.

Entanglement is a key principle of quantum teleportation. It enhances entanglement configuration through the use of precomputed entangled states, consistent channel fidelities, and optimized synchronization, facilitating accelerated and scalable simulations. Although these shortcuts enhance performance, they limit physical layer fidelity, so slightly limiting accuracy in hardware-level modeling. Set up an entanglement is required for the initial configuration of teleportation as shown in Fig. 5. Getting the qubit q_z ready to teleport to Y, implement Hadamard's Gate on q_z.

$$H(|\phi\rangle_z) = \frac{1}{\sqrt{2}}(|0\rangle_z + |1\rangle_z) \tag{9}$$

$$|\phi\rangle_z = H(|\phi\rangle_z) \otimes |00\rangle_{XY} = \frac{1}{\sqrt{2}}(|0\rangle_z + |1\rangle_z) \otimes |00\rangle_{XY} \tag{10}$$

Use CNOT gates

$$|\phi\rangle_z = \text{CNOT}(q_z, q_x) \cdot |\phi\rangle_z = \frac{1}{\sqrt{2}}(|00\rangle_{XZ} + |11\rangle_{XZ}) \otimes |0\rangle_Y \tag{11}$$

$$|\phi\rangle_z = \text{CNOT}(q_z, q_y) \cdot |\phi\rangle_z \tag{12}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle_{XZ} \otimes |0\rangle_Y + |11\rangle_{XZ} \otimes |1\rangle_Y) \tag{13}$$

X classically communicates the measurement findings to Y as outcome x and outcome y after measuring the entangled qubits q_x and q_y. Y applies the Pauli-X gate on q_z if outcome $x = 1$. If outcome $y = 1$, Y gives q_z the Pauli-Z gate. q_z is in the condition of $|\phi\rangle_z$ as X originally prepared after Y makes the adjustments determined by x's measurement results. q_z has therefore been transferred from X to Y.

It allows quantum state propagation without qubit relocation. The speed of teleportation is constrained by conventional transmission, which in turn leads to delays when covering long distances. Due to its complexity and resource needs, challenges arise while scaling the process. The inefficiency of quantum teleportation stems from the fact that to transmit only one qubit, two classical bits are transmitted.

Superdense coding protocol is incorporated here because it can greatly enhance the effectiveness of transmitting data by utilizing entangled qubits, resulting in an overall improved efficiency in quantum protocols for communication. It is a quantum communication technique that enables the communication of two classical bits of information with a single qubit. Long-distance quantum networks can regulate decoherence time during teleportation and superdense coding by implicitly adding time-dependent state evolution into quantum operation sequences. Sequential operations indirectly address teleportation decoherence time limitations. Time parameter to reflect state degradation across long distances could improve fidelity within practical limits. A decay function can regulate superdense coding decoherence by tracking state fidelity loss over distance. SO-ERA$_{Sim}$ facilitates time synchronization between classical and quantum message channels. Superdense coding across multiple hops topologies through sequential operation, with quantum state transfers and classical decoding implicitly coordinated. The entanglement-based routing solution proposes multi-hop participation. Getting Started with an entangled set of the qubits q_x and q_y created by host X and Y.

$$|q_x, q_y\rangle = |00\rangle \tag{14}$$

X applies hadamard gate on q_x.

$$H(|0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{15}$$

$$|q_x, q_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{16}$$

A CNOT gate is applied on q_x as the control qubit and q_y as the target qubit.

$$CNOT(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{17}$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{18}$$

The next step is encoding the message, which requires X to apply a certain set of quantum gates to the first qubit in a way that allows a 2-bit message to be encoded. No gate is applied to the message "0", so the state remains unchanged.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{19}$$

Pauli X gate is applied on message "01", which flips the state of the qubit as X|0⟩=|1⟩,X|1⟩=|0⟩.

$$X|\Phi^+\rangle = X\left(\frac{1}{2}(|00\rangle + |11\rangle)\right) = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \tag{20}$$

A Pauli Z gate is applied on message "10" adding a phase flip as

$$Z|0\rangle = |0\rangle \quad \text{and} \quad Z|1\rangle = -|1\rangle \tag{21}$$

$$Z|\Phi^+\rangle = ZX\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right) = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \tag{22}$$

A Pauli Z and X gate are applied on message "11"

$$ZX|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \tag{23}$$

Now, host (X) will transmit qubit q_x to Y. Y decrypts the message by performing a quantum operation on the qubit he received as q_x and his own qubit q_y.

With q_x as acting and q_y as target qubit, Y performs the CNOT gate operation.

$$\text{CNOT}(|\Phi^+\rangle) = \text{CNOT}\left(\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)\right) \tag{24}$$

$$= \frac{1}{\sqrt{2}}(|11\rangle - |01\rangle) \tag{25}$$

Now Y will apply a hadamard gate on q_x.

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{26}$$

The condition of Message "11" becomes

$$H\left(\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)\right) = \frac{1}{\sqrt{2}}((|0\rangle - |1\rangle) + (|1\rangle - |0\rangle)) \tag{27}$$

Y measures both qubit q_x and q_y to extract the 2-bit classical message. The measured classical bits correspond to the encoded message from X. This protocol uses quantum entanglement to facilitate efficient communication. Despite its theoretical benefits, superdense coding has some significant practical constraints. Decoherence and noise make it difficult for the transmitter and receiver to maintain a mutually entangled state over long distances. However, it is not feasible to expand the protocol to cover huge networks and connect them to pre-existing communication networks. Its utilization is hindered by security issues such as side-channel assaults. SO-ERA$_{Sim}$ analyzes entanglement reliability in dynamic node switching or teleportation chaining using density matrix overlap and stabilizer based syndrome metrics. It employs dynamic entanglement purification when fidelity falls below a threshold to maintain integrity and records results in a shared database, but frames in the code suggest a simulated implementation.

As the methods given have some limitations, new methods have been introduced as hybrid protocols. By integrating the best features of both quantum and classical approaches, hybrid protocols improve scalability and security while making large-scale secure communication more efficient and feasible. It is advantageous for practical quantum communication due to its reduced reliance on entanglement, increased error resilience, scalability, flexibility, and ability to utilize classical communication infrastructure. These attributes make hybrid protocols more robust, flexible and practical for real-world applications than existing superdense coding protocols. By ensuring the successful execution of unit tests, assertion validations, and analytical comparison between simulation results and theoretical metrics such as reliability and failure rate, SO-ERA$_{Sim}$ preserves protocol fidelity. Furthermore, performance analysis and parameter optimization are employed to mitigate deviations, ensuring the simulator's behavior adheres to formal quantum protocol specifications.

7.2. Hybrid quantum-classical protocol

The hybrid protocol between host X and host Y begins with entanglement-based QKD. At the beginning, X and Y both have a qubit that is in the state of $|0\rangle$. A Hadamard gate (H) is used by host X to convert its qubit into a superposition state.

$$H|0\rangle_X = \frac{1}{\sqrt{2}}(|0\rangle_X + |1\rangle_X) \tag{28}$$

The following step involves a CNOT gate operation, in which X and Y will execute to entangle their qubits. Consequently, the outcome is as follows:

$$\text{CNOT}\left(\frac{1}{\sqrt{2}}(|0\rangle_X + |1\rangle_X)|0\rangle_Y\right) = \frac{1}{\sqrt{2}}(|00\rangle_{XY} + |11\rangle_{XY}) \tag{29}$$

X then randomly chooses a series of classical bits ($0 or 1$) to encode into a quantum state and prepares 10 qubits accordingly. If the bit is 1, using the Pauli-X gate switches the state to $|1\rangle$.

$$X|0\rangle = |1\rangle \tag{30}$$

Applying a Hadamard gate on a chosen basis of 1 leads to forming a superposition.

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{31}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{32}$$

Y receives qubits from X, and measures each qubit on the standard or diagonal (superposition) chosen by X after receiving them. Contrasted with diagonal basis measurements, which distinguish between $|0\rangle$ and $|1\rangle$, rectilinear basis measurements distinguish between:

$$\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\} \tag{33}$$

After that, X and Y communicate information about bases to the public. They combine the remaining results into a common key and ignore the ones where their bases do not match. This key is built using the results of the corresponding measurements i.e shared_key = comparing results X encrypts the message using the XOR method after determining the shared key:

$$\text{Encrypted\_msg}[i] = \text{Message}[i] \oplus \text{key}[i\%\text{len(key)}] \tag{34}$$

Y then uses the same key to perform the XOR operation once more to decrypt the message that was received:

$$\text{Decrypted\_msg}[i] = \text{Encr\_msg}[i] \oplus \text{key}[i\%\text{len(key)}] \tag{35}$$

The protocol detects eavesdropping by using quantum connections and measurements to protect the distribution of keys. The key is used for symmetric encryption to guarantee the message's secrecy.

7.3. SO-ERA$_{Sim}$

By ensuring the efficiency, reliability and resistance to eavesdropping of quantum communication networks, security-oriented entanglement protocols contribute significant success of these networks. The no-cloning theorem and quantum state disturbance are two examples of potential security properties that can be identified and maximized with it. To generate secure cryptographic keys, this approach utilizes entanglement. The essential security benefits of quantum communication are combined with optimization techniques, error correction, adaptive routing, and the efficient utilization of resources in security based entangled routing algorithms.

All network hosts are initiated by start methods. Creating and using an entanglement between the source and destination hosts is the main process for guaranteeing safe communication. To achieve this, entanglement-based routing is employed while secure entanglement is being established. When X and Y work together, they produce a pair of entangled qubits. X and Y generate an entangled pair of qubits by using Hadamard and CNOT gates. The resultant of the given qubit after hadmard operation by Eq. (28) and CNOT operation by Eq. (29).

$$|\psi\rangle_{XY} = \frac{1}{\sqrt{2}}(|00\rangle_{XY} + |11\rangle_{XY}) \tag{36}$$

Security protocols are implemented to guarantee secure communication between X and Y. Typically, this process entails enhancing privacy and rectifying errors. Entanglement swapping employs intermediate hosts to ensure the secure routing of the quantum message. In Entanglement Swapping a qubit X becomes interconnected with qubit Y through an intermediary host, and qubit Y is also tangled with qubit Z.

$$\frac{1}{2}(|00\rangle_{XY} + |11\rangle_{XY}) \otimes (|00\rangle_{YZ} + |11\rangle_{YZ}) \tag{37}$$

final destination:

$$\frac{1}{2}(|00\rangle_{XZ} + |11\rangle_{XZ}) \tag{38}$$

The hosts that act as intermediary to the starting point and final destination are resolute. Turning on Entanglement Swapping keeps the source and destination in an entangled state, and intermediate hosts use measurement to swap the entanglement.

8. Performance evaluation

In this section, experiments are conducted to evaluate the performance of proposed SO-ERA$_{Sim}$ Hybrid protocol and SO-ERANET protocols with state-of-art protocols. We first give a detailed description of the experimental setup and then show the performance of proposed protocols. The SO-ERA$_{Sim}$ Hybrid protocol and SO-ERANET protocol are implemented on a system using an Intel(R) Xeon(R) Gold 6248R CPU operating at a speed of 3.00 GHz (with 2 processors) and 128 GB

Table 2
Metrics of Simulator Protocols: Latency, Throughput, and Error Rate Analysis.

Simulator	Protocol Name	Latency Rate (Sec)	Throughput (Ops/s)	Error Rate (%)
ProjectQ [48]	Teleportation/Superdense	0.102/0.082	–	–
EQSN [49]	Teleportation/Superdense	0.283/0.296	–	–
CQC [19]	Teleportation/Superdense	0.301/0.533	–	–
SO-ERA$_{SIM}$	Hybrid (proposed)	0.3305	111.9378	0.2
SO-ERA$_{SIM}$	SO-ERANET (proposed)	0.03180	31.4368	1.0

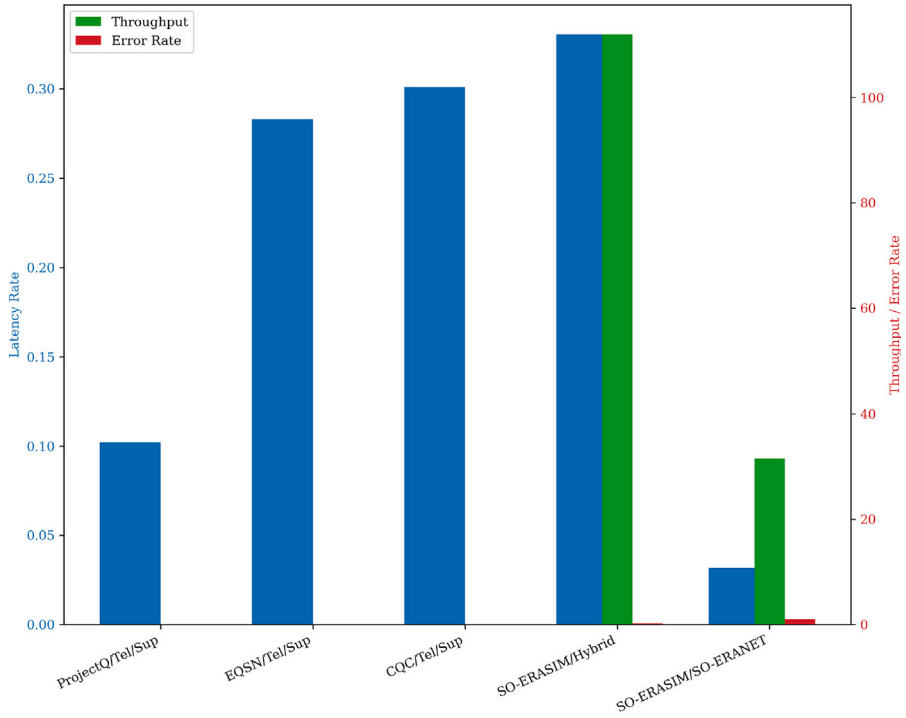

Fig. 6. Performance metrics of quantum simulators and protocols.

of RAM. The system operates on a 64-bit operating system and utilizes Python version 3.12.4.

The simulation results of a quantum network that uses entanglement to guarantee the security and reliability of communications between hosts is shown in Table 2. The simulations cover multiple hosts using different communication methods. Table 2 represents the performance characteristics for each protocol in multiple simulators, including latency rate (measured in operations per second), throughput (also measured in operations per second), and error rate (expressed as a percentage). Each individual host in the network can create and exchange entangled qubits, enabling safe communication with other hosts. SO-ERA$_{Sim}$ implies Markovian quantum noise (such as depolarizing and amplitude damping), constant link failure probabilities, and uniformly distributed gate failures. These assumptions simplify modeling but impact measurements of performance by potentially minimizing fidelity, underestimating latency, and suppressing error rates. Resulting in too optimistic outcomes relative to real-world settings characterized by dynamic noise and hardware variability.

Fig. 6, analyzes quantum simulator performance across protocols in hybrid quantum communication networks. Each chart bar represents a specified simulator-protocol combination. The main indicator is the latency rate, shown by blue bars. Lower values indicate better performance. The secondary y-axis shows throughput (green bars) and error rate (red bars), which is important for data transmission efficiency and dependability. This visualization compare and evaluate simulators such as $ProjectQ$, $EQSN$, CQC, and SO-ERA$_{Sim}$ under multiple protocols (Tel/Sup, Hybrid, SO-ERANET). This research uses performance measures to make recommendations for quantum networking applications.

SO-ERA$_{Sim}$ latency enhances linearly with hop count and protocol complexity, whereas throughput declines with rising qubit storage capacity and node count due to communication and memory overhead. Performance significantly declines above 100 nodes, enabling concurrency approximations to sustain efficiency. It utilizes consistency strategies such as fixed random seeds, predetermined quantum state configurations, and uniform event scheduling to ensure repeated performance assessments. By averaging parameters such as latency, fidelity, and throughput over multiple simulation instances and reporting the standard deviation. Measurement variance is minimized to quantify variability and ensure statistical reliability. It overcomes classical-quantum synchronization issues by timestamping events and integrating coordination latency such as measurement feedback and correction timing into the final processing duration. It analyzes link integrity and latency in real time, utilizing threshold-based triggers to identify performance loss. Upon identification of problems, it dynamically shifts entanglement paths through adaptable routing algorithms and resets internal data to ensure protocol expansion without requiring restart.

This work explores a hybrid quantum communication network that combines six protocols, four of which follow established techniques and two of which are novel approaches: "Hybrid" and "SO-ERA$_{Sim}$". We focus on multihost communication frameworks utilizing OSI layers up to the physical layer. Extensive analysis of latency rate, throughput, and error rate metrics underpins our efforts to optimize data transmission efficiency through iterative protocol refinement. The simulation outlines secure qubit transmission, highlighting the inherent security properties of quantum communication. The hybrid protocol employs a

mix of symmetric keys for classical and quantum computing, strengthening security measures. In contrast, SO-ERA$_{Sim}$ uses entanglement swapping to facilitate information transfer in quantum multihost networks. The unique addressing mechanism during qubit transfer ensures seamless communication between hosts.

9. Conclusion

This study has successfully developed a strategy for a resilient and adaptable simulator in quantum communication protocols. This simulator offers a comprehensive platform for the analysis and evaluation of performance and security-oriented hybrid quantum communication protocols. Our application provides comprehensive statistics on error rates, and protocol efficiency across many contexts, rendering it essential for both researchers and practitioners in the field of quantum communication. User-specified scale models, variable protocol components, and flexible entanglement generation modules allow SO-ERA$_{Sim}$ to evaluate quantum approaches. The modular architecture's flexibility to extend quantum techniques and measurement protocols allows modeling of specialized algorithmic features without affecting the key infrastructure. The simulator's scalability and accuracy are validated by the execution of these six protocols. This sets the basis for future developments and improvements in secure quantum communication systems. It is expected to greatly enhance the advancement and implementation of quantum communication technology, facilitating safer and more efficient data transmission in the quantum age. The centralized event queue, the storage requirements for monitoring quantum states, and the requirement for integrated communication between classical and quantum processes, all limit the scalability of SO-ERA$_{Sim}$. By employing distributed scheduling, abstracting quantum state models, including parallel computing. Enabling asynchronous communication, later iterations may improve scalability.

The layered architecture and modular protocol framework guide the development of future quantum networks and cross-layer stacks by emphasizing the distinction of quantum and classical control, the dynamic management of entanglement routing, and the synchronization of operations across layers. Its event-driven scheduling and fidelity-aware routing logic offer a framework for scalable, real-time control of quantum networks in actual hardware applications.

Future endeavors will concentrate on developing an innovative hybrid protocol that integrates key rate, distance, and efficiency to tackle essential challenges in quantum communication, including scalability and accuracy. Future potential approaches incorporate the integration of teleportation and superdense protocols with hardware to contrast simulated and actual qubit outcomes. The entanglement-based routing approach can connect with network quantum devices through the transmission of qubits for hardware-in-the-loop testing, thereby proving entanglement fidelity.

It ensures consistency via adaptive protocol design, uniform qubit interfaces for versatile interoperability, and seed-controlled allocation for deterministic testing. These characteristics allow experts to further their work through clear abstractions and reliable benchmarks. The design emphasizes "clone-and-run" functionality with low configuration constraints.

CRediT authorship contribution statement

Saumya Priyadarshini: Writing – review & editing, Writing – original draft, Software, Methodology, Investigation, Formal analysis, Conceptualization. **Chandrashekar Jatoth:** Validation, Supervision. **Rajesh Doriya:** Validation, Supervision. **Rajkumar Buyya:** Validation, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] D. Pan, G.-L. Long, L. Yin, Y.-B. Sheng, D. Ruan, S.X. Ng, J. Lu, L. Hanzo, The evolution of quantum secure direct communication: on the road to the qinternet, in: IEEE Communications Surveys & Tutorials, IEEE, 2024.

[2] Y. Xu, T. Wang, P. Huang, G. Zeng, Integrated distributed sensing and quantum communication networks, Research 7 (2024) 0416.

[3] T. Nguyen Hoa, Muhammad Usman, Rajkumar Buyya, iQuantum: A toolkit for modeling and simulation of quantum computing environments, Softw.: Pr. Exp. 54 (6) (2024) Wiley Online Library.

[4] Mitali Sisodia, Manoj Kumar Mandal, Binayak S. Choudhury, Hybrid multi-directional quantum communication protocol, 2024, arXiv preprint arXiv:2402.14043.

[5] N.J. Greybush, V. Pacheco-Peña, N. Engheta, C.B. Murray, C.R. Kagan, Plasmonic optical and chiroptical response of self-assembled au nanorod equilateral trimers, ACS Nano 13 (2) (2019) 1617–1624.

[6] N. Mohammadi Estakhri, B. Edwards, N. Engheta, Inverse-designed metastructures that solve equations, Science 363 (6433) (2019) 1333–1338.

[7] L. La Spada, C. Spooner, S. Haq, Y. Hao, Curvilinear metasurfaces for surface wave manipulation, Sci. Rep. 9 (1) (2019) 3107.

[8] L. La Spada, L. Vegni, Near-zero-index wires, Opt. Express 25 (20) (2017) 23699–23708.

[9] Binjie He, Dong Zhang, Seng W. Loke, Shengrui Lin, Luke Lu, Building a hierarchical architecture and communication model for the quantum internet, 2024, arXiv preprint arXiv:2402.11806.

[10] Shouqian Shi, Xiaoxue Zhang, Chen Qian, Concurrent entanglement routing for quantum networks: Model and designs, in: IEEE/ACM Transactions on Networking, IEEE, 2024.

[11] L. La Spada, L. Vegni, Electromagnetic nanoparticles for sensing and medical diagnostic applications, Materials 11 (4) (2018) 603.

[12] Yuval Idan, Avihai Didi, A review of quantum communication using high-dimensional Hilbert spaces, 2024, arXiv preprint arXiv:2402.01319.

[13] Shraddha Singh, Mina Doosti, Natansh Mathur, Mahshid Delavar, Atul Mantri, Harold Ollivier, Elham Kashefi, Towards a unified quantum protocol framework: Classification, implementation, and use cases, 2023, arXiv preprint arXiv:2310.12780.

[14] Yu-Xiang Xiao, Lan Zhou, Wei Zhong, Ming-Ming Du, Yu-Bo Sheng, The hyperentanglement-based quantum secure direct communication protocol with single-photon measurement, Quantum Inf. Process. 22 (9) (2023) 339, Springer.

[15] I.H. Lee, D. Yoo, P. Avouris, T. Low, S.H. Oh, Graphene acoustic plasmon resonator for ultrasensitive infrared spectroscopy, Nature Nanotechnology 14 (4) (2019) 313–319.

[16] HaoRan Hu, HuaZhi Lun, ZhiFeng Deng, Jie Tang, JiaHao Li, YueXiang Cao, Ya Wang, Ying Liu, Dan Wu, HuiCun Yu, et al., High-fidelity entanglement routing in quantum networks, Results Phys. 60 (2024) 107682, Elsevier.

[17] Manoj Kumar Mandal, Binayak S. Choudhury, Soumen Samanta, Hybrid bidirectional quantum communication protocol of two single-qubit states under noisy channels with memory, Quantum Inf. Process. 22 (11) (2023) 406, Springer.

[18] Ryosuke Satoh, Michal Hajdušek, Naphan Benchasattabuse, Shota Nagayama, Kentaro Teramoto, Takaaki Matsuo, Sara Ayman Metwalli, Poramet Pathumsoot, Takahiko Satoh, Shigeya Suzuki, et al., Quisp: a quantum internet simulation package, in: 2022 IEEE International Conference on Quantum Computing and Engineering, QCE, IEEE, 2022, pp. 353–364.

[19] Stephen DiAdamo, Janis Nötzel, Benjamin Zanger, Mehmet Mert Beşe, Qunetsim: A software framework for quantum networks, IEEE Trans. Quantum Eng. 2 (2021) 1–12, IEEE.

[20] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpędek, M. Skrzypczyk, L. Wubben, Netsquid, a network simulator for quantum information using discrete events, Commun. Phys. 4 (1) (2021) 164.

[21] R. Jha, D. Das, A. Dash, S. Jayaraman, B.K. Behera, P.K. Panigrahi, A novel quantum N-queens solver algorithm and its simulation and application to satellite communication using IBM quantum experience, 2018, arXiv preprint arXiv:1806.10221.

[22] Xiaoliang Wu, Alexander Kolar, Joaquin Chung, Dong Jin, Tian Zhong, Rajkumar Kettimuthu, Martin Suchara, SeQUeNCe: a customizable discrete-event simulator of quantum networks, Quantum Sci. Technol. 6 (4) (2021) 045027, IOP Publishing.

[23] Rishab Chatterjee, Kaushik Joarder, Sourav Chatterjee, Barry C. Sanders, Urbasi Sinha, QkdSim, a simulation toolkit for quantum key distribution including imperfections: Performance analysis and demonstration of the B92 protocol using heralded photons, Phys. Rev. Appl. 14 (2) (2020) 024036, APS.

[24] Axel Dahlberg, Stephanie Wehner, SimulaQron—a simulator for developing quantum internet software, Quantum Sci. Technol. 4 (1) (2018) 015001, IOP Publishing.

[25] Mario Mastriani, Quantum key secure communication protocol via enhanced superdense coding, Opt. Quantum Electron. 55 (1) (2023) 10, Springer.
[26] Yiming Zeng, Jiarui Zhang, Ji Liu, Zhenhua Liu, Yuanyuan Yang, Entanglement routing design over quantum networks, in: IEEE/ACM Transactions on Networking, IEEE, 2023.
[27] L. Zhou, B.W. Xu, W. Zhong, Y.B. Sheng, Device-independent quantum secure direct communication with single-photon sources, Phys. Rev. Appl. 19 (1) (2023) 014036.
[28] Jatin Khurana, An ultimate benchmark for the optimal performance of quantum communication network using multi path routing protocol, in: 2023 World Conference on Communication & Computing, WCONF, IEEE, 2023, pp. 1–7.
[29] Gowri T. Sridhar, P. Ashwini, Nikhath Tabassum, A review on quantum communication and computing, in: 2023 2nd International Conference on Applied Artificial Intelligence and Computing, ICAAIC, IEEE, 2023, pp. 1592–1596.
[30] Devendar B. Rao, Ramkumar Jayaraman, A novel quantum identity authentication protocol without entanglement and preserving pre-shared key information, Quantum Inf. Process. 22 (2) (2023) 92, Springer.
[31] Syed Rakib Hasan, Mostafa Zaman Chowdhury, Md Saiam, Yeong Min Jang, Quantum communication systems: vision, protocols, applications, and challenges, IEEE Access (2023) IEEE.
[32] Yiyou Fan, Zhang Zaichen, Simple quantum communication protocol based on bell test, in: 2022 14th International Conference on Wireless Communications and Signal Processing, WCSP, IEEE, 2022, pp. 826–830, http://dx.doi.org/10.1109/WCSP55476.2022.10039287.
[33] Mario Mastriani, Quantum key secure communication protocol via enhanced superdense coding, Opt. Quantum Electron. 55 (1) (2023) 10, Springer.
[34] Arindam Dutta, Anirban Pathak, Controlled secure direct quantum communication inspired scheme for quantum identity authentication, Quantum Inf. Process. 22 (1) (2022) 13, Springer.
[35] Xiaoxue Zhang, Ri-Gui Zhou, An efficient and novel semi-quantum deterministic secure quantum communication protocol, Internat. J. Theoret. Phys. 61 (4) (2022) 94, Springer.
[36] Yuan Lee, Eric Bersin, Axel Dahlberg, Stephanie Wehner, Dirk Englund, A quantum router architecture for high-fidelity entanglement flows in quantum networks, Npj Quantum Inf. 8 (1) (2022) 75, Nature Publishing Group UK London.
[37] Y.A. Chen, Q. Zhang, T.Y. Chen, W.Q. Cai, S.K. Liao, J. Zhang, K. Chen, J. Yin, J.G. Ren, Z. Chen, S.L. Han, An integrated space-to-ground quantum communication network over 4 600kilometres, Nature 589 (7841) (2021) 214–219.
[38] Rodney Van Meter, Ryosuke Satoh, Naphan Benchasattabuse, Kentaro Teramoto, Takaaki Matsuo, Michal Hajdušek, Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, A quantum internet architecture, in: 2022 IEEE International Conference on Quantum Computing and Engineering, QCE, IEEE, 2022, pp. 341–352.
[39] F.K. Asadi, S.C. Wein, C. Simon, Long-distance quantum communication with single 167Er ions, 2020, arXiv preprint arXiv:2004.02998.
[40] J. Janis Notzel, Stephen DiAdamo, Entanglement-enhanced communication networks, in: 2020 IEEE International Conference on Quantum Computing and Engineering, QCE, IEEE, 2020, pp. 242–248.
[41] Yong Yu, Fei Ma, Xi-Yu Luo, Bo Jing, Peng-Fei Sun, Ren-Zhou Fang, Chao-Wei Yang, Hui Liu, Ming-Yang Zheng, Xiu-Ping Xie, et al., Entanglement of two quantum memories via fibres over dozens of kilometres, Nature 578 (7794) (2020) 240–245, Nature Publishing Group UK London.
[42] Wojciech Kozlowski, Axel Dahlberg, Stephanie Wehner, Designing a quantum network protocol, in: Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies, 2020, pp. 1–16.
[43] Takaaki Matsuo, Clément Durand, Rodney Van Meter, Quantum link bootstrapping using a RuleSet-based communication protocol, Phys. Rev. A (2019).
[44] T. Jones, A. Brown, I. Bush, et al., QuEST and high-performance simulation of quantum computers, Sci. Rep. 9 (2019) 10736, http://dx.doi.org/10.1038/s41598-019-47174-9.
[45] Axel Dahlberg, Matthew Skrzypczyk, Tim Coopmans, Leon Wubben, Filip Rozpdek, Matteo Pompili, Arian Stolk, Przemysaw Pawe czak, Robert Knegjens, Julio de Oliveira Filho, et al., A link layer protocol for quantum networks, in: Proceedings of the ACM Special Interest Group on Data Communication, 2019, pp. 159–173.
[46] Yuan Cao, Yongli Zhao, Qin Wang, Jie Zhang, Soon Xin Ng, Lajos Hanzo, The evolution of quantum key distribution networks: On the road to the qinternet, IEEE Commun. Surv. Tutor. 24 (2) (2022) 839–894, IEEE.
[47] Stefano Pirandola, End-to-end capacities of a quantum communication network, Commun. Phys. 2 (1) (2019) 51, Nature Publishing Group UK London.
[48] D.S. Steiger, T. Häner, M. Troyer, ProjectQ: An open source software framework for quantum computing, Quantum 2 (2018) 49, http://dx.doi.org/10.22331/q-2018-01-31-49.
[49] B. Zanger, S. DiAdamo, EQSN: Effective quantum simulator for networks, 2020, [Online]. Available: https://github.com/tqsd/EQSN_python.