Secure and Efficient Entanglement Distribution Protocols for Near-Term Quantum Internet

Nicholas Skjellum[§], Mohamed Shaban[§,†] and Muhammad Ismail[§]
[§]Department of Computer Science, Tennessee Technological University, Cookeville, TN, USA
[†]Department of Mathematics, Faculty of Education, Alexandria University, Egypt
Emails: {nskjellum42, mmibrahims42, mismail}@tntech.edu

***Abstract*—Quantum information technology has the potential to revolutionize computing, communications, and security. To fully realize its potential, quantum processors with millions of qubits are needed, which are still far from being accomplished. Thus, it is important to establish quantum networks to enable distributed quantum computing to leverage existing and near-term quantum processors into more powerful resources. This paper proposes an efficient entanglement distribution protocol for classical-quantum networks with a limited number of quantum links, enabling quantum teleportation in near-term hybrid networks. The proposed protocol uses entanglement swapping and classical network coding to distribute entanglements efficiently while overcoming bottlenecks and minimizing qubit and link usage. Experimental results show that the proposed protocol requires quantum resources that scale linearly with network size, with individual nodes only requiring a fixed number of qubits. For small network sizes of up to three transceiver pairs, the proposed protocol outperforms the benchmark by using 17% fewer qubit resources, achieving 8.8% higher accuracy, and with a 35% faster simulation time. The percentage improvement increases significantly for large network sizes. We also propose a protocol for securing entanglement distribution against malicious entanglements using quantum state encoding through rotation. Our analysis shows that this method requires no communication overhead and reduces the chance of a malicious node retrieving the teleported state to 7.2%. The achieved results point toward a protocol that enables a highly scalable, efficient, and secure near-term quantum Internet.**

***Index Terms*—Quantum networks, quantum teleportation, entanglement distribution, entanglement swapping, quantum Internet.**

I. Introduction

QUANTUM information technology represents a key enabler to new applications within computing, communications, sensing, intelligence, and security. However, the world's most powerful quantum processor, the IBM Osprey [1], has only 433 qubits, with the second most powerful processor, the IBM Eagle [2], having only 127 qubits. To effectively realize the applications of quantum computing, a processor that holds millions of qubits is necessary, which is far from being accomplished with current technology. To harness the potential of quantum computing in the near future, a quantum Internet capable of connecting multiple quantum processors across large distances is necessary to enable distributed quantum computing in place of singular quantum processors. To facilitate this near-term implementation of distributed quantum networks, we expect that early versions of this quantum Internet will consist of hybrid classical-quantum networks, with central node or groups of nodes connected to all other quantum devices through optical fiber network links (compatible with quantum and classical communications), with the remaining devices connected through the classical Internet. In this paradigm, quantum teleportation [3], a technique that utilizes classical bits to transmit quantum states, can be used to allow these quantum devices to exchange quantum states without having a direct quantum-compatible link. However, to utilize quantum teleportation, entanglements [3] are required. Entanglements must be generated locally within a single device (central node or nodes), with the entangled states then distributed to all devices participating in the quantum teleportation. As a result, the means to create, distribute, and exploit these entanglements in an efficient manner are integral to the development of a quantum Internet [4].

To optimize the advantages of teleportation within this hybrid network, the efficient utilization of the limited number of quantum links is paramount for entanglement distribution. In instances where direct quantum links between nodes are unavailable, nodes must utilize alternative paths through the network for distributing entanglements, frequently leading to bottlenecks along paths shared by multiple communicating parties. As a result, teleportation throughput is constrained across all communicating nodes. Moreover, the challenges associated with the limited coherence time of qubits introduce a critical time constraint. This constraint underscores the significance of addressing bottlenecks in quantum networks, as the distribution of entanglement pairs becomes a pressing concern before decoherence renders them useless. Therefore, this work aims to enhance the efficiency of entanglement distribution within a constrained network by applying parallelism. We demonstrate our solution on a butterfly network for ease of visualization, but it can just as effectively be used within a more complex network.

Additionally, as these entanglements are distributed through the network, individual devices within the network may be untrusted, but by necessity must participate to complete the distribution. Consider a scenario where a malicious node is expected to assist in distributing a quantum entanglement by transferring an entangled state to a designated transmitter. In this scenario, the malicious node desires the contents of a state the transmitter will send. This malicious node can compromise the security of the transmitter by introducing its own entanglement, which it has full control over, in an attack

known as a malicious entanglement [5]. By transferring this malicious entangled state, whenever the sender and receiver communicate by teleportation, the malicious device will be able to eavesdrop on the teleported quantum state without issue as long as it is able to discover the two-bit classical teleportation message that will retrieve the state, or otherwise with a 25% probability of recovering it through a random guess. As quantum teleportation will be used frequently within the near-term network to allow indirectly connected quantum devices to communicate, this attack poses a significant threat. In addition, as the classical message that is used to recover the teleported quantum state is only two bits long, encrypting it with existing classical methods is wasteful, as it incurs a significant overhead for a limited gain in security. Instead, it is more efficient to encode the quantum states being teleported. This paper aims to develop an efficient and secure entanglement distribution protocol that overcomes bottleneck links to enable an optimal teleportation rate between indirectly connected quantum devices.

A. Related Works

Min et al. [6] and Wang et al. [7] use quantum network coding to facilitate the preparation of multi-qubit and qudit states respectively between indirectly connected nodes. Qu et al. [8] utilize quantum network coding to reduce noise within communicated messages. Rall et al. [9] propose a method for distributing measurement-based entanglements by creating a fully entangled butterfly network. However, each of these works require the existence of a full optical fiber-connected network in order to perform quantum network coding, making them incompatible with our ideal near-term hybrid quantum Internet. Beaudrap et al. [10] propose specific network structures that provide greater efficiency for such a network but does address throughput limits because of bottlenecks.

For securing quantum communication, authors such as Song et al. [11] forgoes classical communications and utilizes only quantum information, which makes it inapplicable for near-term hybrid classical-quantum networks. Another proposal from Kato et al. [12] approaches quantum security by only allowing unidirectional communication, which does not require the distribution of entanglements, but also requires a full quantum network.

Much of the existing literature does not address entanglement distribution on classical-quantum networks, nor do their solutions scale efficiently even when distributing quantum states. Alternative configurations fail to provide a general solution that can be employed in any network configuration. Further, the security solutions presented in the literature are only applicable to quantum-only communications and are prohibitive when used to protect the entanglement distribution or otherwise make it difficult to perform.

For general entanglement distribution, several works attempted to distribute entanglement across indirectly connected nodes. For instance, Sutcliffe et al. [13] introduce a method to establish GHZ-states (entanglements of more than two qubits) between indirectly connected nodes using only shared Bell pairs [3]. Li et al. [14] demonstrate a communication protocol using entangled qubits to facilitate communication across any network structure but fails to address the issue of bottlenecks. Lastly, Herbert [15] proposes a protocol that seeks to overcome bottleneck links while supporting entanglement distribution between indirect nodes, and is implemented in a classical-quantum network. We utilized Herbert's protocol as a benchmark to evaluate the efficiency of our proposed solution as it distributes entanglements in parallel and its final entangled states are strictly Bell pairs.

B. Contributions

To support a near-term quantum Internet on a classical-quantum network we contribute the following:

- We propose an entanglement distribution protocol, Indirect Entanglement Distribution with Teleportation Coding (IEDTC), that overcomes network bottlenecks. This protocol is capable of distributing multiple entanglements within the same network between multiple transceiver pairs (which consist of a transmitter and receiver node) simultaneously and allows for quantum teleportation of quantum states between indirectly connected nodes within the network.
- We propose a security protocol, Quantum State Rotation Encoding (QSRE), to protect against eavesdropping through malicious entanglements by encoding quantum states through state rotation. Any state encoded this way can only be retrieved by correctly performing an inverse operation on the modified state. Encoding the quantum state only requires reading from a pre-shared private key that is not exposed by encoding the quantum state. In addition, the proposed protocol does not impose any overheads on the information being transferred, since no additional classical bits are added to the teleportation message.
- We implement the IEDTC and QSRE protocols in a quantum network simulator, QuNetSim [16], and provide the results from our experiments. We compare IEDTC with the protocol proposed by Herbert [15] to benchmark our protocol's efficiency, accuracy, and resource requirements. Simulation results show that IEDTC outperforms the benchmark, utilizing 17% fewer qubit resources while achieving an 8.8% increase in accuracy and demonstrating a 35% reduction in simulation time. We also analyze the security of QSRE by evaluating the success rate of a malicious receiver attempting to retrieve a quantum state encoded using QSRE. Simulation results show that QSRE reduces the chance of a malicious node retrieving the teleported state to 7.2%.

The rest of this paper is as follows. Section II presents the network model. Section III presents our IEDTC protocol. Section IV presents our QSRE protocol. Section V provides the simulation results and discussions on their significance. Section VI concludes the paper and includes our future work.

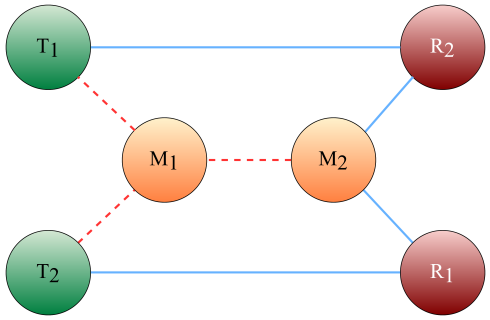

Fig. 1: Butterfly classical-quantum network: Blue connections represent optical fiber links and red connections represent classical links. The link between M_1 and M_2 is the bottleneck link.

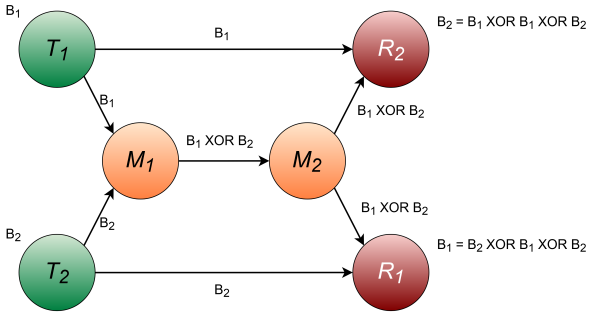

Fig. 2: Illustration of classical network coding to increase the throughput when there is a network bottleneck

II. System Model

Consider a hybrid classical-quantum network, composed of nodes. In our model, a node is an abstract computer which has access to classical and quantum computational resources. Within this model, a pair of nodes wish to communicate, but have no direct links through which to send information to each other. The only means available to these nodes requires transmitting information through indirect paths between them within the network, along which other nodes are simultaneously sending information at the same time. If the bandwidth needed from these common links exceeds their capabilities, communications slow down, and the efficiency of the network is reduced. To visualize this problem, we utilize a butterfly network. The butterfly network consists of a set of transmitter nodes, each denoted by T_n, and receiver nodes, each denoted by R_n, with each T_n and R_n paired together and referred to as a transceiver pair. In this network, neither node of any transceiver pair is directly connected with one another. We define the network entities below, with a visual reference in Fig. 1 for a network of size two (i.e., 2 $T_n - R_n$ pairs).

- Each transmitter T_n is connected to all receivers in the network, except R_n, through optical fiber links.
- Each transmitter T_n is connected to a central node M_1 via a classical link. Each transmitter T_n is a source of entangled states.
- Each receiver R_n is connected to a central node M_2 via an optical fiber link. M_2 is a source of entangled states.
- The central nodes M_1 and M_2 are connected through a classical link, which represents the network bottleneck.

For classical messages, classical network coding [17], depicted in Fig. 2, is employed to circumvent the network bottleneck by sending multiple classical messages B_n simultaneously through the same middle link between M_1 and M_2. Each transmitter broadcasts its message to all connected receivers and M_1. Then, M_1 XORs all the messages into a single string and sends it to M_2. M_2 broadcasts this string to each receiver. Finally, each receiver recovers the original message sent by its transmitter pair by XORing the string sent by M_2 with the messages received from each directly connected transmitters, hence, recovering B_n.

When teleporting quantum states, two steps are required: (1) distributing entanglements between each transmitter-receiver pair and (2) exchanging classical teleportation messages between each transmitter-receiver pair to recover the teleported state. For the classical messages (step 2), classical network coding can be used to overcome the bottleneck between M_1 and M_2. However, classical network coding techniques cannot be applied when distributing the entangled quantum pairs through the bottleneck between M_1 and M_2 (step 1) due to no-cloning theorem [3]. Hence, we aim to develop a protocol to distribute the entangled states while overcoming the bottleneck.

III. IEDTC: Proposed Indirect Entanglement Distribution with Teleportation Coding Protocol

This section introduces our protocol for entanglement distribution across network bottlenecks. IEDTC utilizes entanglement swapping and quantum teleportation to transmit quantum states. Entangled pairs are generated in a central node and in each transmitter. Pair halves are then distributed to connected receivers. These receivers perform entanglement swapping to provide each transmitter with an entangled state that is shared by the transmitter's target receiver. With entanglements established between transceiver pairs, quantum states are delivered using quantum teleportation, which transmits a classical message from the transmitter to its paired receiver. Here, classical network coding is used to efficiently transmit multiple teleportation messages and to avoid the network bottleneck. Without loss of generality, the following example demonstrates the protocol on a network of size two, as depicted in Fig. 3. The same principles are applied for networks of larger sizes.

1) Transmitter T_1 creates an entangled pair $|\phi_1\rangle = |\phi_{11}\rangle |\phi_{12}\rangle$ and sends half of it ($|\phi_{11}\rangle$) to R_2. Similarly, transmitter T_2 creates an entangled pair $|\phi_2\rangle = |\phi_{21}\rangle |\phi_{22}\rangle$ and sends half of it ($|\phi_{21}\rangle$) to R_1.
2) Central node M_2 creates two entangled pairs, $|\psi_1\rangle = |\psi_{11}\rangle |\psi_{12}\rangle$ and $|\psi_2\rangle = |\psi_{21}\rangle |\psi_{22}\rangle$. Then, M_2 distributes the halves of $|\psi_1\rangle$, sending $|\psi_{12}\rangle$ to R_1 and $|\psi_{11}\rangle$ to R_2.

Similarly, it distributes the halves of $|\psi_2\rangle$ and sends $|\psi_{21}\rangle$ to R_1 and sends $|\psi_{22}\rangle$ to R_2.

3) Node R_1 now holds $|\phi_{21}\rangle$ (entangled with T_2), $|\psi_{12}\rangle$ (entangled with R_2), and $|\psi_{21}\rangle$ (entangled with R_2). Then, R_1 consumes $|\phi_{21}\rangle$ to teleport $|\psi_{21}\rangle$ to T_2, thus performing entanglement swapping. Now, T_2 and R_2 are entangled. In this step, R_1 is serving as an entanglement swapping node for T_2 and R_2.
4) Likewise, R_2 holds $|\phi_{11}\rangle$ (entangled with T_1), $|\psi_{11}\rangle$ (entangled with R_1), and $|\psi_{22}\rangle$ (entangled with R_1). Then, R_2 consumes $|\phi_{11}\rangle$ to teleport the quantum state $|\psi_{11}\rangle$ to T_1, performing an entanglement swap as well. Now, T_1 and R_1 are entangled. In this step, R_2 is serving as an entanglement swapping node for T_1 and R_1.

As shown in Fig. 3, a given receiver $R_{n'}$ will assist in entangling an adjacent receiver R_n, where $n \neq n'$, with its transmitter pair T_n. In a general setting, Fig. 4 depicts the expanded relationship for a network of size N. Each receiver entangles an adjacent receiver with its paired transmitter, and this receiver in turn is entangled with its paired transmitter by another receiver. Each receiver distributes entanglements in parallel with all other receivers thus increasing the efficiency of the protocol. Also, the independence of each distributed entanglement allows central node M_2 to distribute entanglements on demand rather than as a batch; this reduces the resource requirements of this node. Entanglement distribution for larger networks is defined in Algorithm 1.

Algorithm 1 IEDTC Entanglement Distribution Sub-protocol for a network of size N

Entanglement Distribution Sub-protocol

Require: $N \geq 2$

Establish N sets of nodes, where each set consists of a T_n, R_n, and $R_{n'}$, where $n \neq n'$.

A receiver will be an R_n in one set, and an $R_{n'}$ in another.

for all $R_n, R_{n'}$ **do**

M_2 creates entangled pair ($|\psi_{n1}\rangle$, $|\psi_{n2}\rangle$), then distributes them.

$R_{n'} \leftarrow |\psi_{n1}\rangle$

$R_n \leftarrow |\psi_{n2}\rangle$

end for

for all T_n **do**

T_n creates entangled pair ($|\phi_{n1}\rangle$, $|\phi_{n2}\rangle$), then sends $|\phi_{n1}\rangle$ to $R_{n'}$.

$R_{n'} \leftarrow |\phi_1\rangle$

end for

for all $R_{n'}$ **do**

$R_{n'}$ entanglement swaps $|\psi_{n1}\rangle$ to T_n using entangled pair ($|\phi_{n1}\rangle$, $|\phi_{n2}\rangle$).

$T_n \leftarrow |\psi_{n1}\rangle$ ▷ The qubit containing $|\phi_{n2}\rangle$ now contains $|\psi_{n1}\rangle$.

end for ▷ Each transceiver pair (T_1, R_1) now contains an entanglement between both nodes.

With entanglements distributed, each transceiver pair ($T_n - R_n$) holds half of an entangled pair, which is then used to perform quantum teleportation of any state $|\eta_n\rangle$. As part of teleportation (step 2 discussed in Section II), a two-bit classical string B_n is created, with classical network coding used to transmit this teleportation message. To do so, each transmitter T_n performs a Bell measurement [3] on its shared entangled state and the qubit containing $|\eta_n\rangle$, generating B_n. Then, each transmitter broadcasts its teleportation message to all connected receivers and M_1. Next, M_1 will combine all teleportation messages it receives into a single classical message using a logical-XOR operation, then transmit this combined message to M_2.M_2 broadcasts this message to all receivers. Each receiver then subtracts each teleportation message $B_{n'}$ it received from each transmitter $T_{n'}$ from the combined message through additional XOR operations between each $B_{n'}$ and the combined message. This recovers B_n, which R_n uses as control values for quantum gates to retrieve $|\eta_n\rangle$. Using our proposed entanglement distribution approach based on M_2 and classical network coding based on M_1, transceiver pairs can perform teleportation while overcoming the bottleneck link $M_1 - M_2$ and the limited number of quantum links. This process is generalized in detail in Algorithm 2.

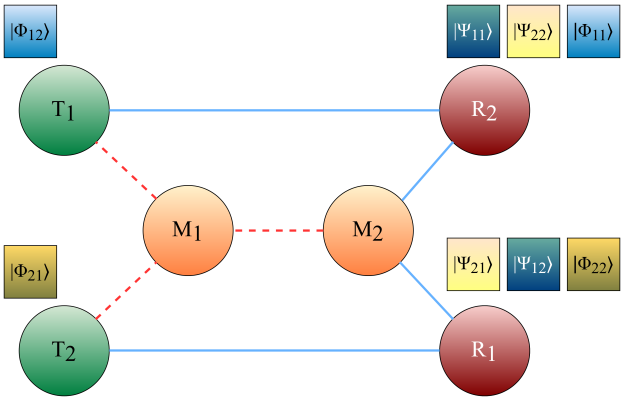

Fig. 3: Entangled states prior to entanglement swapping

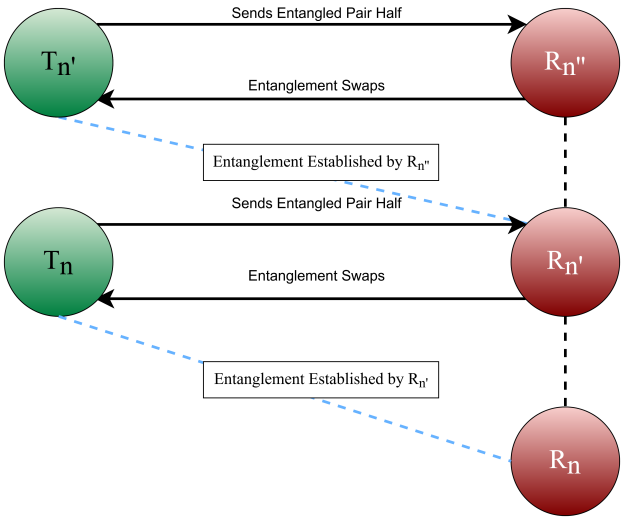

Fig. 4: Relationships between receivers in a larger network

Algorithm 2 IEDTC Teleportation Sub-Protocol for network size N

Teleportation Coding Sub-protocol

Require: $N \geq 2$

for all T_n **do**

T_n will prepare a quantum state $|\eta_n\rangle$, which they will teleport to R_n using the shared entanglement $|\psi_n\rangle(|\psi_{n1}\rangle, |\psi_{n2}\rangle$).

T_n will perform a bell measurement on η_n and its half of the entanglement $|\psi_{n1}\rangle$, creating a classical message C_n, which we call the teleportation message.

T_n will broadcast the teleportation message C_n to all $R_{n'}$ and M_1.

end for

M_1 will collect all teleportation messages C_n, then combine them into a single classical message C_N using a logical XOR operation, which it will transmit to M_2.

M_2 will broadcast C_N to all receivers R_n.

for all R_n **do**

R_n will receive C_N and $N-1$ teleportation messages $C_{n'}$. Using a logical XOR, it will subtract each $C_{n'}$ from C_N, recovering C_n.

R_n will apply the teleportation message C_n to the quantum gates used to retrieve the teleported state and retrieve $|\eta_n\rangle$.

end for

A. Benchmark Protocol

To establish a benchmark to compare our protocol against we also implemented the protocol outlined by Herbert [15], as it addresses similar issues of entanglement distribution to overcome network bottlenecks. We chose this protocol as a benchmark for two reasons: (a) it establishes entanglements between nodes that cannot directly communicate with each other in both directions and (b) it specifically is designed for a hybrid classical-quantum network, which is depicted in Fig. 5. This network is a modified butterfly network, as defined in Section II, with the following modifications:

- Each transmitter T_n is connected to the receiver R_n through a directed quantum (optical fiber) link from T_n to R_n. The receiver cannot send any information to the transmitter through this link.
- Each transmitter T_n is connected to each other transmitter $T_{n'}$ through a directed classical link.
- Central node M_2 is connected to receiver R_n through a directed classical link.

IV. QSRE: Proposed Security Protocol

When quantum network nodes are inherently trusted, the network becomes vulnerable to attacks by eavesdroppers that desire to acquire quantum states transmitted within the network. To perform this eavesdropping, a malicious receiver R_n, which is connected to transmitter $T_{n'}$ by a direct link, attempts to acquire a quantum state that would originally be

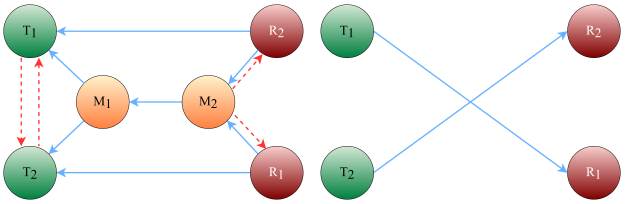

Fig. 5: Network connections of benchmark [15]. Links within this network are defined with specific directions: Red links are classical. Blue links are optical fiber

teleported to $R_{n'}$. To do this, the malicious receiver R_n creates a malicious entangled pair and transmits half of the malicious entangled pair to $T_{n'}$. Instead of sharing an entanglement with $R_{n'}$, $T_{n'}$ now shares an entanglement with the malicious receiver R_n. This attack is known as malicious entanglement [5]. In this situation, the malicious node is easily capable of retrieving the quantum states teleported by $T_{n'}$. Because of the nature of our proposed protocol, R_n will directly receive the teleportation message used to retrieve $\eta_{n'}$ as part of the quantum teleportation protocol, guaranteeing the attacker will be able to discover any teleported information. This jeopardizes (a) the privacy of the network, since no quantum state is safe from being eavesdropped, (b) the availability of the network, since $R_{n'}$ is unable to retrieve a quantum state whenever a malicious receiver eavesdrops on quantum states, and (c) the integrity of the network, because any information $R_{n'}$ receives is not usable for further computation.

To combat eavesdropping resulting from malicious entanglement, we introduce QSRE to secure teleported quantum states without applying any overhead to the classical communications used to transmit the teleportation message. A quantum state is described as being on the surface of the Bloch sphere [3]. By rotating a quantum state on this sphere, we can encode the quantum state without increasing the overhead of the teleportation message used to retrieve the quantum state. Even if a malicious receiver were to acquire the rotated state, it would still need to guess the inverse of the rotation performed on the original quantum state. Assuming that R_n and T_n are sharing a private key S_n, we outline the encoding process below:

1) A node T_n wants to teleport a quantum state $|\eta_n\rangle$. Before teleporting this state, the transmitter T_n will read the ith $2+D$ bits from a pre-shared private key S_n that it shares with R_n, where i is the message number in a round of communications, and D is the number of bits used to reflect the degrees of rotation.
2) T_n will use the first bit to rotate in either the X-axis or Y-axis, with a 0 rotating the state around the X-axis, and 1 the Y-axis. T_n will then use the second bit to determine the direction, negative or positive, of this rotation.
3) The last D bits will be used to determine the angle of rotation, using the following equation: $\theta = \frac{\pi}{-1^b \times (1+d)}$, where b is the value of the second bit used to determine the direction of the rotation, and d is the decimal value

of the D bits. For example, if the bits read from the private key were 1011, the quantum state would be rotated around the Y-axis, in the negative direction, with a decimal value of d evaluating to three.

4) Once rotated, the quantum state $|\eta_n\rangle$ will become $|\eta'_n\rangle$, which will then be teleported. To recover $|\eta_n\rangle$, R_n will retrieve $|\eta'_n\rangle$, then read the same ith bits from its shared private key S_n and perform the inverse of the rotation performed by T_n, recovering $|\eta_n\rangle$.

For a malicious receiver to recover $|\eta_n\rangle$, it must guess the axis of rotation, the direction, and the magnitude of the rotation angle θ. The ideal (lowest) success rate of a malicious receiver attempting to defeat this method is $\frac{1}{2^{D+2}}$. Also, encoding a quantum state in this manner reveals no information from the private key to an eavesdropper, thereby allowing key reuse. By integrating IEDTC with QSRE, secure and efficient teleportation can be accomplished across hybrid classical-quantum networks with limited quantum links and overcome their resource bottlenecks.

V. Results and Discussion

To assess the performance of IEDTC and QSRE in QuNetSim [16], the following metrics have been considered. For IEDTC and the benchmark protocol [15], we examined qubit usage, the number of links required for the network of a given network size N, the simulation time, and the accuracy of the protocol when noise was introduced to the network.

To calculate qubit usage, we analyzed the maximum number of distinct qubits required by the protocol. For the purposes of our experiment, this is equivalent to the greatest number of quantum states held by each participating node from any given time period in the protocol. The number of links required by each protocol is determined by the number of network connections across the entire network between nodes. We also distinguish between classical-only links and quantum links when comparing these requirements.

Simulation time is the time required for the protocol to be completed within QuNetSim by our implementation, consisting of entanglement distribution and quantum teleportation phases with IEDTC and QSRE. Accuracy is the success rate of a protocol when quantum gates had an $X\%$ chance to introduce noise.

A. Setup

QuNetSim was configured within an Ubuntu distribution for the Windows Linux Subsystem using the backend EQSN [18] that was provided with QuNetSim. The environment was run with 16 cores with a speed per CPU of 24.2 GhZ. To check for errors in quantum states, EQSN was modified to provide state vectors of qubits within the network. To implement noise, the backend was modified so that quantum gates would introduce noise with a variable rate determined before the experiment began. Increasing this rate made it more likely a gate would perform a noise-introducing version of its typical function. This function would transform the state accordingly based on the type of quantum gate called but would introduce noise to the quantum state by modifying the state values that were operated on by a small amount. An increase to this rate made it more likely a gate would introduce noise in this manner. Accuracy was tested over a range from 1% to 10% chance for a gate to introduce noise when utilized. Network size was determined by the number of transceiver pairs ($T_n - R_n$) within the network. The benchmark implementation of Herbert's protocol [15] had a limited network size, with sizes larger than 3 not possible because of a memory exception raised by the numpy library: "*numpy.core._exceptions._ArrayMemoryError*," with QuNetSim requiring a two-dimensional array of float64 integers of 512 gigabytes to simulate a network size of 4, with requirements increasing for larger network sizes. We did not have a machine capable of providing this amount of memory for our simulations and were thus unable to test the benchmark for network sizes greater than 2.

TABLE I: Resource usage comparison between IEDTC and benchmark [15] per entanglement distribution. N is the size of the network in terms of the number of transmitter-receiver pairs.

Protocol	Total Number of Links	Number of Quantum Links	Number of Qubits
Benchmark[15]	$3N^2+5N+2$	$2N^2+5N+2$	$2N^2+3N+1$
IEDTC	N^2+N+1	N^2	$7N$

B. IEDTC Results

Table I shows the resource usage in terms of the number of qubits and required links. Both protocols required a quadratic increase in the number of links as network size increased. However, IEDTC used fewer links in comparison because of its more lenient network requirements. Further, the benchmark's qubit usage also quadratically increased while IEDTC only utilized a linearly increasing supply of qubits to distribute the same number of entanglements. IEDTC required on average 17% fewer qubits to establish entanglements and transmit messages across the network. The link usage of both protocols is depicted in Fig. 6, while the increase in qubit usage is depicted in Fig. 7.

To test accuracy, each protocol was run over $1,000$ trials at each noise probability. A trial's success required all states to be correctly received, any incorrect states resulted in a failed trial. We determined correctness by comparing the original and transmitted quantum states from each trial. Successes and failures were averaged for each level of noise with a 95% confidence interval. Fig. 8 compares the accuracy of both protocols. Experiments show that IEDTC and the benchmark [15] had comparable accuracy at a network size two, but IEDTC performed with better accuracy at a network of size three. Two factors contributed to this. First, the benchmark utilizes an extensive entanglement containing all qubits within the network, with any noise introduced propagated to all other quantum states. Second, the greater number of qubits

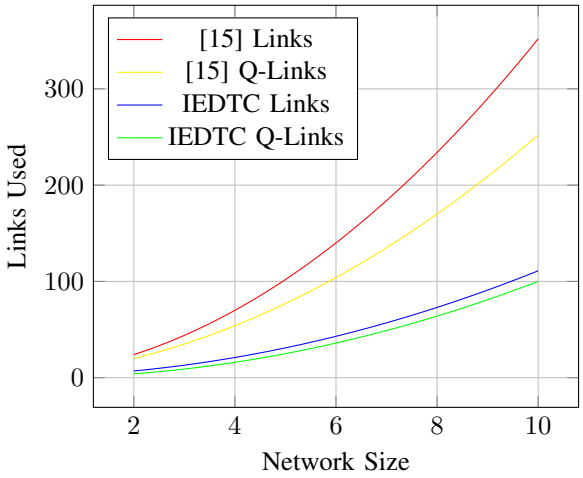

Fig. 6: Link usage of IEDTC and benchmark [15]

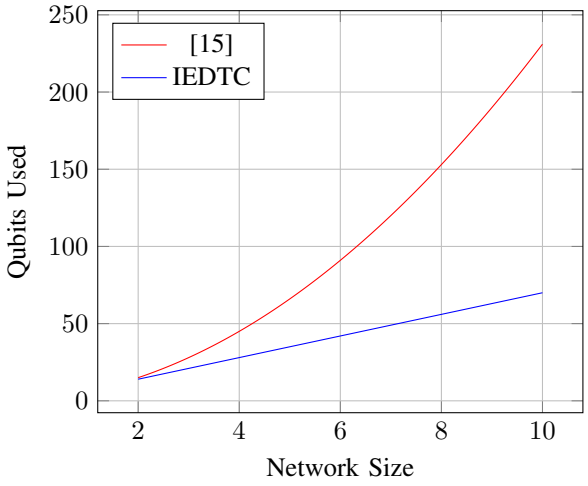

Fig. 7: Qubit usage of IEDTC and benchmark [15]

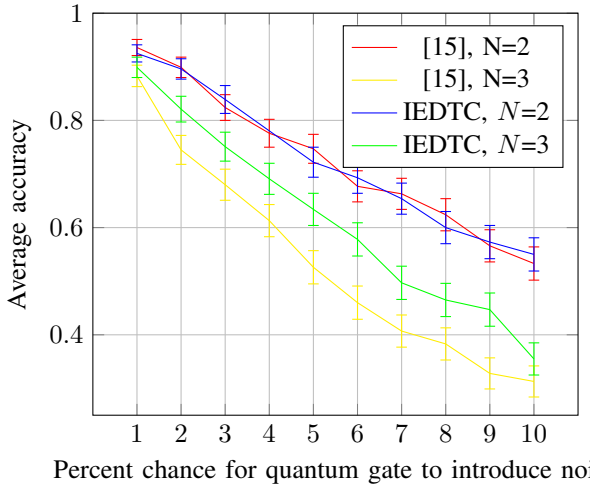

Fig. 8: Accuracy of IEDTC and benchmark [15]

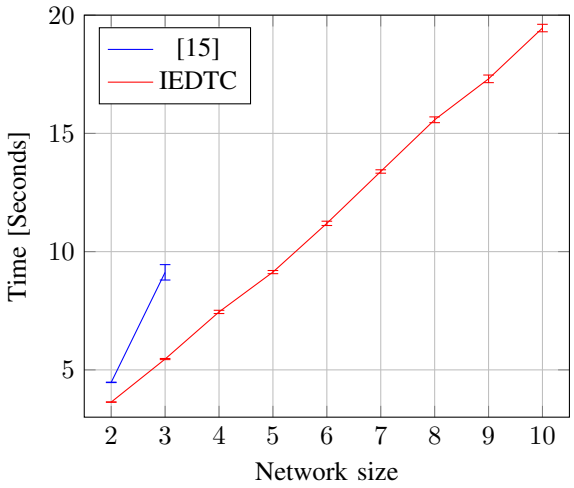

Fig. 9: Simulation time of IEDTC and benchmark [15]

within the benchmark at network of size three required more quantum operations to distribute entanglements, providing more chances for a gate operation to introduce noise. In IEDTC, any error introduced was contained to a specific entanglement. Error in one entanglement would not affect the quantum states of other entanglements, resulting in IEDTC performing with an greater average accuracy at network size three. For larger network sizes, we would expect IEDTC to continue to outperform the benchmark.

Fig. 9 shows the time taken in simulation to distribute and teleport quantum states by both IEDTC and the benchmark [15]. Simulation time was calculated by averaging the runtime of both protocols over 100 iterations within 95% confidence interval. IEDTC surpassed the benchmark, achieving an overall 35.2% faster simulation time. The benchmark utilizes a comparable number of qubits at network size two, but at this size it requires a greater number of quantum operations, limiting its efficiency. When distributing entanglements, the benchmark transmits $N \times (N-1)$ qubits at startup and cannot continue until all of these qubits reach their destination. As such, the protocol is unable to serve individual entanglements and must distribute them in batches, requiring quantum memory to do so. IEDTC, in comparison, establishes individual entanglements in parallel. M_2 and each T_n transmit their required states synchronously to the target receiver, minimizing the need for quantum memory and utilizing parallelism. IEDTC performs with greater efficiency compared to the benchmark when distributing and teleporting states.

C. QSRE Results

A network of size two was prepared for testing the effectiveness of QSRE, with two transceiver pairs and one malicious receiver. In Fig. 10, four bits read (two bits for direction and sign and two bits for the angle θ) from the shared key was sufficient to achieve the lowest probability of 7.2% for guessing how to decode the quantum state, with further bits from five onward increasing the chance of the attacker's success.

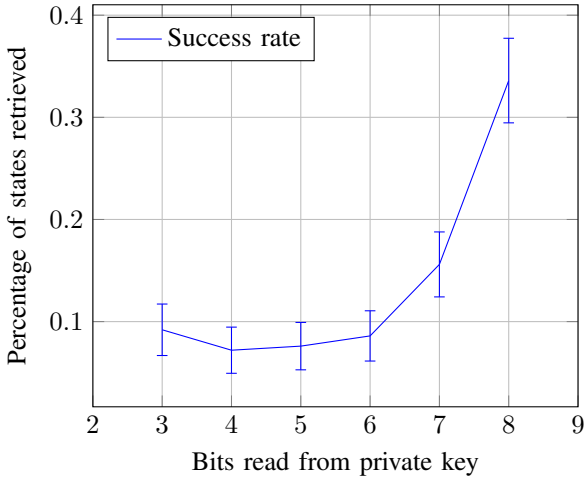

Fig. 10: Success rate of eavesdropper decoding quantum state Network size is 2.

From the original equation $\theta = \frac{\pi}{-1^b \times (1+d)}$, increasing the number of bits to determine the value of d provides more possible angles that the quantum state can be rotated by. However, this results in an increased number of rotations with a reduced magnitude of rotation. When decoding the quantum state, adjacent bit values would result in the return of effectively the same quantum state, introducing false positives in favor of the malicious receiver acquiring a correct state. This rate increases significantly as further bits are used to determine the angle θ, resulting in an increased chance of success for the malicious node.

To reduce the success rate of the malicious receiver further, the initial value used within our equation for the angle θ can be increased from π to a greater value such as 2π. For a rotation around a sphere, π is only the equivalent of $\frac{1}{4}$ of the available rotation around the sphere in a specific direction. By increasing this initial value, we can theoretically introduce additional D when determining θ, further lowering the success rate of the malicious receiver.

VI. Conclusions

This paper proposes IEDTC, an entanglement distribution and quantum teleportation protocol that can distribute entangled pairs between indirectly connected nodes and avoid bottlenecks that would reduce the teleportation throughput. To accomplish this, IEDTC distributes entanglements by entanglement swapping, and then utilizes quantum teleportation with classical network coding. By using classical links and a limited number of quantum links to exchange quantum states, we enable near-term classical-quantum networks for distributed quantum computing. To gauge our performance, IEDTC and a state-of-the-art benchmark were implemented in QuNetSim. Simulation results demonstrate that IEDTC requires fewer qubits and network links, achieves greater efficiency and accuracy, and also scales better than the benchmark.

To support the security of IEDTC against malicious entanglement attacks, we proposed QSRE. As encrypting a two-bit teleportation message has a maximum gain of $\frac{1}{4}$ to guess the original message, we instead proposed encoding the teleported quantum state through angular rotation. QSRE successfully lowered the success rate of a malicious receiver eavesdropping on this state without incurring additional overhead, the only requirement being a pre-shared private key for each transceiver pair. Because the key's contents are not leaked through the encoding process, transceiver pairs can continue using the same key while communicating with each other.

While the IEDTC protocol as currently implemented succeeds at overcoming the limits of the network, we would be interested in implementing a version with further parallelism, in addition to operating within a network of increased size. At demonstrated, IEDTC relies on a median node to distribute states in a linear order. For more complex networks, other methods of parallel distribution might be investigated to improve this performance at scale. For QSRE, a greater degree of rotation can be permitted when encoding the quantum state, increasing the secrecy possible for teleported quantum states.

VII. Acknowledgements

This work was performed with support from the National Science Foundation under Award #221025. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] Nov 2022. [Online]. Available: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

[2] Nov 2021. [Online]. Available: https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[4] S. Shi and C. Qian, "Concurrent entanglement routing for quantum networks: Model and designs," in *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, ser. SIGCOMM '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 62–75. [Online]. Available: https://doi.org/10.1145/3387514.3405853

[5] T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdušek, and R. V. Meter, "Attacking the quantum internet," *IEEE Transactions on Quantum Engineering*, vol. 2, pp. 1–17, 2021.

[6] J. Min, Z. Shuai, and D. MengXiao, "Quantum network coding based on remote state preparation of arbitrary two-qubit states," in *2017 36th Chinese Control Conference (CCC)*, 2017, pp. 9757–9760.

[7] X. Wang, C. Chen, M. Jiang, and X. Huang, "Quantum network coding for remote state preparation of multi-qudit states," in *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, 2019, pp. 1150–1153.

[8] Z. Qu, Z. Zhang, and Z. Cheng, "Anti-noise quantum network coding protocol based on bell states and butterfly network model," in *Artificial Intelligence and Security*, X. Sun, Z. Pan, and E. Bertino, Eds. Cham: Springer International Publishing, 2019, pp. 56–67.

[9] H. Rall and M. Tame, "Demonstration of teleportation across a quantum network code," 2022. [Online]. Available: https://arxiv.org/abs/2210.02878

[10] N. d. Beaudrap and S. Herbert, "Quantum linear network coding for entanglement distribution in restricted architectures," *Quantum*, vol. 4, p. 356, Nov. 2020. [Online]. Available: https://doi.org/10.22331/q-2020-11-01-356

[11] S. Song and M. Hayashi, "Secure quantum network code without classical communication," *IEEE Transactions on Information Theory*, vol. 66, no. 2, pp. 1178–1192, 2020.

[12] G. Kato, M. Owari, and M. Hayashi, "Single-shot secure quantum network coding for general multiple unicast network with free one-way public communication," *IEEE Transactions on Information Theory*, vol. 67, no. 7, pp. 4564–4587, 2021.

[13] E. Sutcliffe and A. Beghelli, "Multiuser entanglement distribution in quantum networks using multipath routing," *IEEE Transactions on Quantum Engineering*, vol. 4, pp. 1–15, 2023.

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

[15] S. Herbert, "Increasing the classical data throughput in quantum networks by combining quantum linear network coding with superdense coding," *Phys. Rev. A*, vol. 101, p. 062332, Jun 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.101.062332

[16] S. DiAdamo, J. Nötzel, B. Zanger, and M. M. Beşe, "Qunetsim: A software framework for quantum networks," *IEEE Transactions on Quantum Engineering*, 2021.

[17] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[18] S. DiAdamo, J. Nøtzel, B. Zanger, and M. M. Beşe, "Effective quantum simulator for networks (eqsn)," *Github Repository*, 2020.