Implementation of Quantum Secure Direct Communication on NetSquid Simulator

Saw Nang Paing, Wook Park, and Hyundong Shin
Department of Electronics and Information Convergence Engineering
Kyung Hee University, Yongin-si, 17104 Korea
Email: hshin@khu.ac.kr

***Abstract*—Quantum Secure Direct Communication (QSDC) provides an effective solution for secure communication by facilitating the direct transmission of information without the necessity for prior key distribution. To properly implement QSDC in practical quantum networks, it is essential to evaluate its performance in realistic conditions affected by various quantum noise and channel impairments. This study implements the QSDC protocol on the NetSquid simulator to meticulously examine its performance under prevalent cghannel noise scenarios, such as depolarizing, dephasing, amplitude damping and phase damping noises. Our analysis highlights insight for the practical implementation of QSDC, providing a thorough comprehension of its feasibility and robustness against quantum noise.**

I. Introduction

The growing prevalence of cyber threats aimed at sensitive information has highlighted the urgent necessity for strong and secure communication systems. Quantum cryptographic techniques, like quantum key distribution (QKD) protocol, provide a means to securely produce a shared key between the sender and receiver. However, a critical vulnerability remains: should an eavesdropper obtain this shared key, the security of the transmitted information could be compromised. Quantum Secure Direct Communication (QSDC) has emerged as a promising solution that leverages quantum mechanics concepts to improve communication security.

QSDC provides a framework enabling direct communication between the sender and receiver, eliminating the necessity for prior key distribution or encryption. By leveraging quantum properties like entanglement [1] and superposition, QSDC guarantees that any effort by an eavesdropper to overhear or manipulate the communication results in detectable errors, immediately alerting the parties to a potential berach. Thus, it ensures the integrity and secrecy of transmitted data, rendering QSDC a pivotal advancement in secure communications, particularly in environments where information security is paramount. Various QSDC protocols have been proposed so far, including two step process, device-independent nethod, counterfactual approach, those utilizing continuous variables, and so on [2]–[5].

To advance QSDC towards practical implementation in real-world quantum networks, it is imperative to meticulously simulate its performance under realistic conditions. In this study, we employ NetSquid (Network Simulator for Quantum Information using Discrete Events) to evaluate the performance of the QSDC protocol. NetSquid provides a comprehensive platform for simulating quantum communication networks, enabling accurate modeling of quantum processes, devices, and noise effects [6]. The implementation of QSDC within the NetSquid framework facilitates the realization of the protocol in practical quantum network scenarios, which are influenced by factors such as quantum noise and decoherence. This simulation method is essential for comprehending the behaviour of the protocol in environments where practical quantum network constraints are relevant, offering critical insights for enhancing QSDC in forthcoming quantum communication systems.

The rest of the paper is arranged as follows. Sec II delineates the operation of standard QSDC protocol. In Sec II-A, the performance of the protocol is analyzed under different types of channel noise using the NetSquid simulator. Finally, Sec III concludes our work.

II. Standard QSDC

In the standard QSDC protocol, Alice first needs to prepare L numbers of Einstein-Podolsky-Rosen (EPR) pairs, with each pair $|\eta_0\rangle$ in one of the states $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$:

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{\mathrm{mc}} + |11\rangle_{\mathrm{mc}}\right)$$
$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle_{\mathrm{mc}} + |10\rangle_{\mathrm{mc}}\right) \quad (1)$$

where m and c denote the checking and message qubits respectively. This protocol is a two-step process. The first step involves the transmission of checking qubits from Alice to Bob. When Bob receives these qubits from Alice, they verify the security of the first transmission process by randomly selecting k_1 pairs, announcing the positions of the selected pairs, performing measurements, and publicly announcing the results. If no eavesdropping is identified and the error rate remains acceptable during this procedure, Alice proceeds to encode her messages $s_{1i}s_{2i} \in \{00, 01, 10, 11\}$ by applying $\boldsymbol{X}^{s_{1i}}\boldsymbol{Z}^{s_{2i}}$ on her remaining $(L - k_1)$ home qubits where $i = \{0, 1, \ldots, L - k_1 - 1\}$. The state of the each EPR pair after the encoding by Alice is

$$|\eta_1\rangle = \boldsymbol{X}^{s_{1i}}\boldsymbol{Z}^{s_{2i}} \otimes \boldsymbol{I}\,|\eta_0\rangle\,. \quad (2)$$

In the second step, Alice transmits the message qubits to Bob. Similar to the first security check, they randomly select k_2 pairs from the $(L - k_1)$ pairs and verify the secure transmission. If it is confirmed to be secure, Bob performs Bell

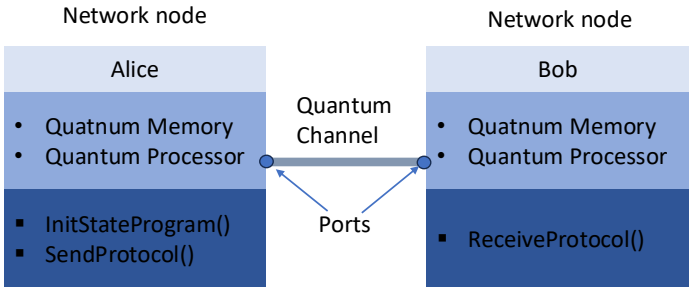

Fig. 1. Modeling of QSDC protocol in NetSquid simulator

state measurement (BSM) by applying a CNOT operation on the message qubit (as the control) and the checking qubit (as the target), followed by applying a Hadamard gate ($\boldsymbol{H}$) to the message qubit on the remaining $(L-k_1-k_2)$ pairs. Bob then decodes the messages $s_{1i}s_{2i}$ by measuring the qubits in the computational basis.

A. Implementation and Results

To assess the performance of the standard QSDC protocol in practical scenarios, we implement it using the NetSquid simulator as depicted in Fig 1. In this simulation, the network, composed of Alice and Bob, is modeled using a modular architecture consisting of distinct components and physical models. Both Alice and Bob are equipped with quantum processors to execute essential quantum operations, such as qubit initialization, gate manipulations, and measurements. Protocols such as 'SendProtocol' and 'ReceiveProtocol' are assigned to these nodes to define their operational behavior. A direct quantum link is established between Alice and Bob to facilitate the transmission of checking qubits and message qubits, which occurs in a two-step process.

Alice prepares EPR pairs using the 'InitStateProgram'. For simplicity, we leave out the EPR pairs that are used for security checking. The transmission of qubits is handled by the 'SendProtocol', which orchestrates the transmission of qubits between nodes within the quantum network. This protocol first initializes and encodes the message qubits via the quantum processor, temporarily storing them in the node's quantum memory. Subsequently, the qubits are transmitted one by one through a quantum channel to the receiving node. After each transmission, the protocol awaits acknowledgment from the receiving node, and upon receipt, discards the acknowledgment qubit before proceeding with the next transmission.

At Bob's end, qubit reception is managed by the 'ReceiveProtocol', which listens on a specified port for incoming qubits. Each qubit is received sequentially in a loop, with Bob generating and sending an acknowledgment qubit back to Alice after each successful reception. Once all qubits are received, they are stored in Bob's quantum memory for future processing. Upon completing the reception of all qubits, the protocol sends a success signal, indicating that the transmission process is complete. Once Bob has successfully received and decoded all the messages sent by Alice, the process concludes.

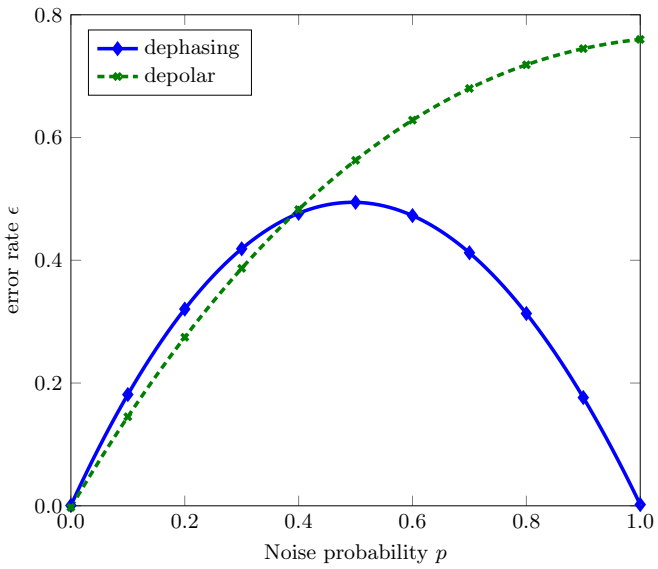

Fig. 2. Error rate ϵ in the presence of dephasing (blue line) and depolarizing (green line) noises with probabity p.

During the qubit transmission, we impose two types of channel noise (depolarizing and dephasing noises).

Depolarizing Noise: Depolarizing noise is regarded as one of the most detrimental types of quantum noise, as it replaces the quantum state of a qubit with a maximally mixed state with probability of p. In practical fiber-based quantum communication channels, this form of noise may arise from imperfections in the transmission medium, including scattering or signal attenuation in optical fibers. In NetSquid, depolarizing noise is modeled using the DepolarNoiseModel, which is applied to qubits being transmitted through a quantum channel.

Dephasing Noise: Dephasing noise affects the phase of the quantum state of a qubit with a certain probability p, leading to the loss of coherence without affecting the energy level of the qubit. In NetSquid, ite is modeled using the DephaseNoiseModel.

To evaluate the performance of the protocol under noisy channels, we calculate the error rate as

$$\epsilon = \frac{n_{\text{errors}}}{n_{\text{total}}}, \tag{3}$$

where ϵ denotes the error rate, n_{errors} represents the number of discrepancies between Alice's encoded message and Bob's decoded message in the sampling EPR pairs, and n_{total} represents the total number of sampling pairs used for the message transmission. For the simulation, we set $n_{\text{total}} = 20$ and execute it over numerous independent iterations to gather statistical data, which is used to evaluate performance of the network. As shown in Fig 2, both types of noise has a profound impact on the QSDC protoocol as a small degree of these noise can lead to significant errors in the transmitted qubits.

III. Conclusions

We have implemented the QSDC protocol on the NetSquid simulator. To assess the performance of the protocol, depolarizing and dephasing noise were introduced to the quantum channel, and the error rate was calculated under these noisy conditions. Our simulation results provide insights into how environmental factors and quantum noise models affect the secure transmission of information. These results can direct future developments in the application of the protocol in practical quantum communication networks.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (NRF-2022R1A4A3033401), the MSIT (Ministry of Science and ICT), Korea, under the Convergence security core talent training business support program (IITP-2024-RS-2023-00266615) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation), and Kyung Hee University in 2023 (KHU-20233663).

References

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Rev. Mod. Phys.*, vol. 81, no. 2, pp. 865–942, Jun. 2009.

[2] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Phys. Rev. A*, vol. 68, p. 042317, Oct. 2003.

[3] L. Zhou, Y.-B. Sheng, and G.-L. Long, "Device-independent quantum secure direct communication against collective attacks," *Sci. Bull.*, vol. 65, no. 1, pp. 12–20, Jan. 2020.

[4] S.Srikara, K. Thapliyal, and A. Pathak, "Continuous variable direct secure quantum communication using Gaussian states," *Quantum Inf. Process.*, vol. 19, no. 4, pp. 1–15, Mar. 2020.

[5] S. N. Paing, F. Zaman, J. ur Rehman, K. M. Byun, J. Cho, T. Q. Duong, and H. Shin, "Counterfactual quantum protocols for dialogue, teleportation, and comparison," *IEEE Trans. Commun.*, Early Access, 10.1109/TCOMM.2024.3443737.

[6] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpedek, M. Skrzypczyk, L. Wubben, W. de Jong, D. Podareanu, A. Torres-Knoop, D. Elkouss, and S. Wehner, "Netsquid, a network simulator for quantum information using discrete events," *Commun. Phys.*, vol. 4, no. 1, p. 164, Jul. 2021.