A solution for analyzing and evaluating quantum communication networks through simulation

Cao Van Toan*, Dang Tien Sy, Bui Thi Thanh Tam, Trieu Duc Quan,
Nguyen Trung Thanh, Do Doanh Dien, Phan Huy Anh

Institute of Information Technology and Electronics, Academy of Military Science and Technology, 17 Hoang Sam, Nghia Do, Hanoi, Vietnam.

*Corresponding author: caotoanryazan@gmail.com

Received 30 Jul. 2025; Revised 26 Sep. 2025; Accepted 10 Oct. 2025; Published 30 Oct. 2025.

DOI: https://doi.org/10.54939/1859-1043.j.mst.IITE.2025.3-11

ABSTRACT

This paper proposes a comprehensive solution for analyzing and evaluating the performance of quantum communication networks through the use of the open-source simulation software, QuNetSim. This method provides a flexible and cost-effective approach to studying network protocols and parameters prior to hardware implementation. The main content of the paper focuses on modeling realistic factors such as channel loss, noise, and eavesdropping behaviors. The research conducted detailed simulation scenarios with the BB84 and E91 protocols. In particular, a general network scenario, integrating quantum repeaters and teleportation, was analyzed through Fidelity. The results not only confirm the crucial role of repeaters in maintaining long-distance connectivity but also quantify the performance degradation caused by channel loss and eavesdropping. The simulation results also demonstrate that QuNetSim is a powerful tool, enabling researchers to easily build, test, and optimize complex quantum networks, thereby accelerating the transition from theory to practice.

Keywords: Quantum communication; BB84; E91; QuNetSim; Simulation.

1. INTRODUCTION

Quantum networking is a pioneering field in science and technology, reshaping how we envision information transmission and computation. Quantum communication is a unique method of transmitting information using the principles of quantum mechanics, particularly through the use of quantum bits, or qubits. This technique leverages quantum phenomena such as superposition and entanglement to establish secure communication channels that are, in theory, immune to eavesdropping. A quantum network is a network of devices capable of transmitting quantum information and distributing quantum entanglement among them. Before progressing towards the realization of a quantum network, the initial phase requires the development and effective testing of quantum network protocols and applications through simulation tools and software. Recently, there have been many efforts in developing quantum simulation software [1], but many of these focus on quantum computing. In addition, only a few simulation software packages have been developed for quantum networks, such as QuNetSim [2], SimulaQron [3], and SQUANCH [4].

QuNetSim is a Python software package that can be used to simulate quantum networks up to the network layer, making it easier to research and test quantum network protocols across various quantum network configurations and parameters. This source code includes many known quantum network protocols so that users can quickly build simulations and beginners can easily learn to implement their own quantum network protocols.

This paper proposes an approach to analyze and evaluate the parameters of quantum communication networks through simulation using the open-source software QuNetSim. First, it provides an overview of quantum communication networks and the parameters affecting their performance. It then analyzes and evaluates these network parameters through simulation results for different scenarios.

2. QUANTUM COMMUNICATION NETWORKS AND SIMULATION SOFTWARE

2.1. Quantum communication networks

The crucial role of quantum networks in shaping the future of communication and computing, especially in the context of increasing cybersecurity threats and the demand for superior information processing capabilities, is undeniable. Quantum networks are built from specialized components that operate based on fundamental principles of quantum mechanics, such as:

- Superposition: A qubit exists in a spectrum of all possible states between 0 and 1. When we "observe" or "measure" the qubit, it "collapses" into a single basic state, either 0 or 1. The act of measurement alters the qubit's state, which is key to detecting eavesdroppers.

- Entanglement: Two qubits can be specially linked, or "entangled." When two qubits are entangled, their states are always correlated, regardless of the distance between them. Therefore, measuring the state of one qubit allows one to deduce the state of the other.

- No-Cloning theorem: It is impossible to create a perfect copy of an unknown quantum state. This means an eavesdropper (Eve) cannot copy quantum information without destroying the original. This is the physical foundation that ensures the security of quantum communication.

- Heisenberg's uncertainty principle: It is impossible to simultaneously know the exact position and momentum of a particle. The more accurately one quantity is measured, the more information is lost about the other.

The main components of a quantum communication network include quantum nodes, quantum channels, and quantum repeaters:

- Quantum nodes, or quantum processors, are devices capable of performing quantum circuits on a certain number of qubits. They are the endpoints in the network, able to transmit and receive quantum information.

- Quantum channels are the physical media that allow the transmission of qubits between nodes, which can be optical fiber channels or free-space channels.

- Quantum repeaters are essential components for extending the range of quantum communication beyond the inherent signal loss limits in optical fibers [5]. Unlike classical amplifiers, quantum repeaters do not amplify the signal but use techniques like entanglement swapping and quantum memory to maintain the integrity of the quantum signal over long distances.

2.2. Simulation software selection

Today, quantum networking is not just a science fiction concept but is gradually becoming a reality, offering breakthrough solutions to security and computational challenges in the digital age. To accelerate this realization, many simulation and testing steps are necessary. Scientists have made significant efforts to develop simulation software for quantum systems. Most of these are aimed at simulating quantum computation and circuits on various hardware configurations with varying degrees of realism. For quantum networks, some popular open-source simulators currently available are: QuNetSim, SimulaQron, and SQUANCH.

- SimulaQron is a simulator that can be used to develop quantum internet software. It simulates multiple quantum processors located at the end nodes of a quantum network, connected by simulated quantum links. The main purpose of SimulaQron is to simulate the application layer of a network, tasks like routing are left for the user to implement as needed. SimulaQron also provides the ability to run simulations on a distributed system, meaning simulations can be set up to run on multiple computers. However, the SimulaQron source code lacks a solution for synchronizing parties regarding the arrival of qubits. A key difference in QuNetSim is that it adds a synchronization layer. QuNetSim integrates an acknowledgment method when information reaches the recipient. One can write protocols more naturally in a standard way, where one handles incoming information (or its absence) before proceeding. SimulaQron also has hosts with features like sending qubits, setting up EPR pairs, and sending classical information. To simplify the task of developing protocols on top of existing ones, QuNetSim has integrated many tasks such as teleporting qubits, setting up GHZ states, and establishing secret keys using QKD.

- SQUANCH (Simulator for Quantum Networks and Channels) achieves similar functionality to SimulaQron but allows for customization of physical layer properties and error models. It enables the creation of distributed quantum information processing simulations that can be parallelized for more efficient simulation. It is specifically designed for simulating quantum networks to test ideas in transmission protocols and quantum networking. SQUANCH can be used to simulate many qubits and allows users to add their own error models, which creates a more realistic quantum network simulator. SQUANCH also allows for the separation of the quantum and classical networks of a complete network, as well as adding length-dependent noise to the channel. A key difference between SQUANCH and QuNetSim is that in SQUANCH, a node can run one script at a time and cannot run more simultaneously. QuNetSim allows for the development of multi-party protocols sequentially and allows them to run in parallel. Furthermore, synchronization between parties is another potential issue with SQUANCH. QuNetSim provides each host with an addressable quantum memory, so with an ID, they can retrieve a qubit and manipulate it as desired. In SQUANCH, users should initialize their qubits before starting the simulation, whereas with QuNetSim, qubits are initialized at runtime. We believe this adds more flexibility when writing protocols and allows for more natural logic in the code.

Therefore, in this study, the authors chose the open-source software QuNetSim to conduct simulations, analysis, and evaluation of quantum communication networks.

The formula representing a qubit is the foundational formula in QuNetSim. A single qubit is described by a vector in a 2-dimensional Hilbert space:

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

where $|0\rangle$ and $|1\rangle$ are the basis states (equivalent to bits 0 and 1), and α and β are complex numbers called probability amplitudes.

The probability of measuring the qubit in state $|0\rangle$ is $|\alpha|^2$ and in state $|1\rangle$ is $|\beta|^2$ with the normalization condition:

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

To describe more complex systems, especially with noise (mixed states), QuNetSim uses the density matrix ρ. For a pure state $|\psi\rangle$, the density matrix is:

$$\rho = |\,\psi\rangle\langle\psi\,| = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & \beta^2 \end{pmatrix} \tag{3}$$

For the transmission channel, QuNetSim simulates it through probability formulas and operators, where the probability for a qubit to reach its destination is $P_{rec} = 1 - P_{\text{loss}}$ and this is the loss_rate parameter used in the simulations. QuNetSim simulates channel errors by applying error operators to the qubit's density matrix. A common model is the depolarizing channel:

$$\rho_{out} = (1-p)\rho_{in} + p\frac{I}{2} \tag{4}$$

Where: p is the probability of an error occurring; ρ_{in} is the qubit state before the channel; ρ_{out} is the noisy qubit state after the channel; $I/2$ is the maximally mixed state.

For channels simulating the E91 protocol [6], the following Bell test formula is used to calculate the correlation level between Alice's and Bob's measurement results:

$$S=E(a,b)-E(a,b')+E(a',b)+E(a',b') \tag{5}$$

where $E(a,b)$ is the correlation value when Alice measures in basis a and Bob measures in basis b. It is calculated as:

$$E(a,b)=P(+,+|a,b)+P(-,-|a,b)-P(+,-|a,b)-P(-,+|a,b) \tag{6}$$

with $P(i,j|a,b)$: Being the probability that Alice gets result i and Bob gets result j when measuring in bases *a* and *b*. QuNetSim simulates these measurements, collects these probability statistics, and calculates the S value.

The quantum bit error rate (QBER) is a simple statistical formula:

$$QBER = \frac{Number\ of\ mismatched\ qubits}{Total\ number\ of\ qubits\ in\ the\ sifted\ key} \tag{7}$$

After obtaining raw metrics like QBER, the final question is how many secret key bits can be generated. This is based on Shannon's information theory. The length of the final secret key after error correction and privacy amplification can be estimated by a simplified version of the Devetak-Winter bound:

$$L \geq n.\left[1 - h_2(Q) - leak_{pA}\right] \tag{8}$$

Where: n is the length of the sifted key; Q is the QBER; $leak_{pA}$ is the amount of information leaked to Eve, which is removed during the privacy amplification step, this amount is also estimated from QBER; $h_2(Q)$ is the binary Shannon Entropy, representing the amount of information leaked during public error correction. It is calculated by formula (9):

$$h_2(Q) = -Q.\log_2(Q) - (1-Q).\log_2(1-Q) \tag{9}$$

As QBER increases $h_2(Q)$ also increases, reducing the key length L. This formula explains why when QBER exceeds a certain threshold (e.g., 11%), the value in the square brackets becomes negative, and the secure key length (L) becomes 0. This is when Alice and Bob must abort the protocol.

Additionally, another extremely important value that can be used as a metric to evaluate the quality of quantum communication is Fidelity. Fidelity determines the degree of similarity between two quantum states. Its value ranges from 0 to 1. If two quantum states are described by density matrices ρ and σ, the Fidelity formula (Uhlmann-Jozsa) [7] is calculated by expression (10):

$$F(\rho,\sigma) = \left(Tr\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2 \tag{10}$$

where Tr is the trace operation.

Specifically, in the open-source software QuNetSim, we compare the final state received by Bob (which may be a mixed state ρ_final due to noise) with the ideal initial state sent by Alice (a pure state |ψ_ideal⟩). Therefore, the fidelity is calculated by the simplified formula (11):

$$F = \langle \Psi_{ideal} | \rho_{final} | \Psi_{ideal} \rangle \tag{11}$$

In summary, QuNetSim is a very powerful tool for studying quantum networks, where the fundamental equations of quantum physics and information theory are programmed to simulate the behavior of complex quantum communication systems. It not only allows for the simulation of protocols like QKD but also provides the necessary building blocks to design and evaluate the performance of complex systems when transmitting entangled pairs through a chain of quantum repeaters.

3. SIMULATION AND EVALUATION OF QUANTUM COMMUNICATION NETWORKS

To conduct experimental simulations to evaluate the quantum communication network system, we first establish specific simulation scenarios. We use the Python language and the libraries in QuNetSim to simulate situations in a quantum communication network and analyze and evaluate the obtained results.

3.1. Simulating and evaluating the operating principle and eavesdropping detection capability of a quantum communication network via the BB84 QKD protocol [8]

The BB84 protocol, developed by Charles Bennett and Gilles Brassard, operates on a "prepare and measure" approach, utilizing the polarization states of single photons to encode and transmit information. Its security is underpinned by fundamental physical laws such as the No-Cloning theorem and the Heisenberg uncertainty principle, whereby any attempt by an eavesdropper (Eve) to gain information will inevitably alter the state of the quantum particles, thus ensuring their detection.

The specific scenario is that Alice sends 10^5 qubits to Bob through a quantum channel simulated on QuNetSim. We calculate and evaluate the Quantum Bit Error Rate (QBER) as a function of the channel's loss rate and Eve's eavesdropping rate. The simulation software will initialize "Hosts," add them to the network, establish connections, initialize qubits and bases, send qubits from Alice to Eve, set the eavesdropping rate, and transmit to Bob, calculating and evaluating the loss on these channels. At Bob's end, the process of measuring qubits, comparing bases, and calculating QBER based on the parameters of channel loss and Eve's eavesdropping rate takes place.

The block diagram illustrating the simulation scenario is shown in figure 1, and the simulation results are shown in figure 2.

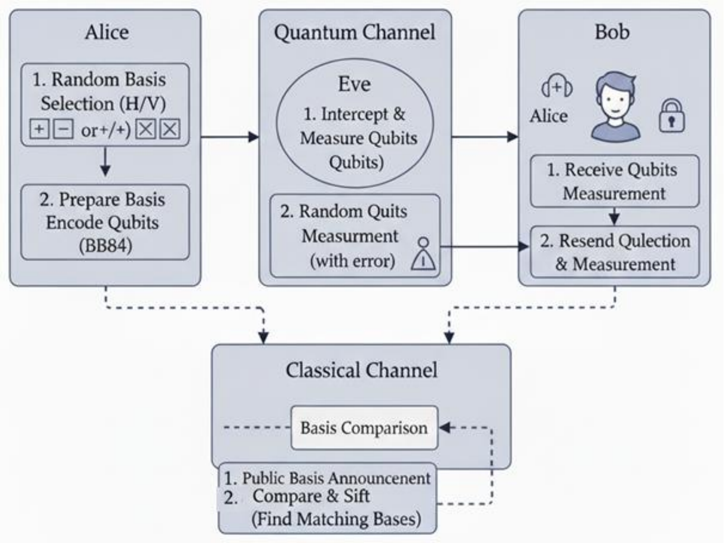
Alice
1. Random Basis Selection (H/V) ⊞⊟ or+/+) ☒☒
2. Prepare Basis Encode Qubits (BB84)
Quantum Channel
Eve
1. Intercept & Measure Qubits Qubits)
2. Random Quits Measurment (with error)
Bob
Alice
1. Receive Qubits Measurement
2. Resend Qulection & Measurement
Classical Channel
Basis Comparison
1. Public Basis Announcenent
2. Compare & Sift (Find Matching Bases)

__Figure 1.__ Block diagram illustrating QKD transmission using the BB84 protocol.

From figure 2, we see that in the case of a channel without eavesdropping, the QBER is almost zero. Thus, QBER is almost independent of the channel loss rate. This is logical because a higher channel loss rate means more qubits are lost during transmission; however, qubit loss does not change the state of the remaining qubits. Therefore, the remaining qubits received by Bob will perfectly match the qubits sent from Alice when measured in the same basis.

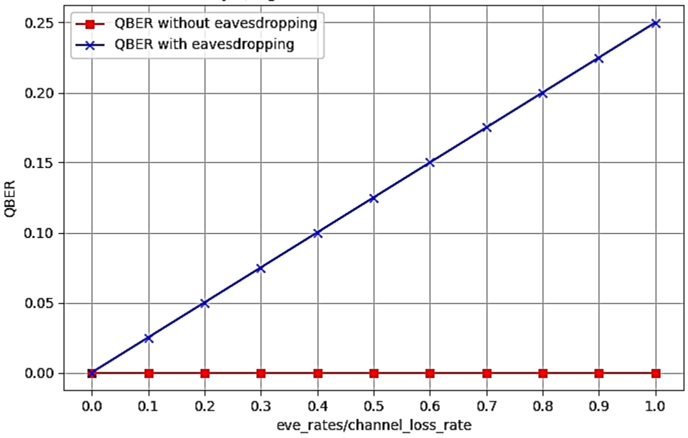

__Figure 2.__ QBER when the channel uses the BB84 protocol.

In the case of eavesdropping on the channel, the graph shows that QBER increases linearly with Eve's eavesdropping rate. This result is fully consistent with the theoretical basis. According to theory, when intercepting a qubit, Eve must randomly choose a basis (rectilinear or diagonal), so the probability of choosing the correct basis and sending the correct qubit to Bob is 50%. At Bob's end, he again randomly chooses a basis to measure this qubit, so there is a 50% chance that Bob will measure the qubit incorrectly. Therefore, an error only occurs when both Eve and Bob choose the wrong basis compared to Alice, and the total error will be 0.5 × 0.5 = 0.25 (25%). Thus, if Eve eavesdrops on 100% of the qubits, the QBER will be about 25%; if she only eavesdrops on 50%, the QBER = 12.5%. From the graph in figure 2, it can be affirmed that the main cause of qubit errors is eavesdropping. Therefore, when QBER exceeds a certain threshold (about 11%) according to formula (9), it can be concluded that the information has been eavesdropped on, and the key exchange must be aborted and a new key transmitted.

3.2. Simulating and evaluating a quantum communication network via the E91 QKD protocol

The E91 protocol is based on a central source creating entangled qubit pairs and sending one qubit of each pair to Alice and the other to Bob. Alice and Bob then randomly choose bases to measure their qubits. The security of the E91 protocol is based not only on comparing qubits like in BB84, but on the correlation level S between Alice's and Bob's measurement results according to formula (5).

When there is no eavesdropping, the qubits remain entangled, and the correlation value S will approach the quantum mechanical limit of $2\sqrt{2}$. When there is eavesdropping, it will break the entanglement, and as a result, the S value will decrease, adhering to the classical physics limit ($|S| \leq 2$). The block diagram illustrating QKD transmission according to the E91 protocol is shown in figure 3.

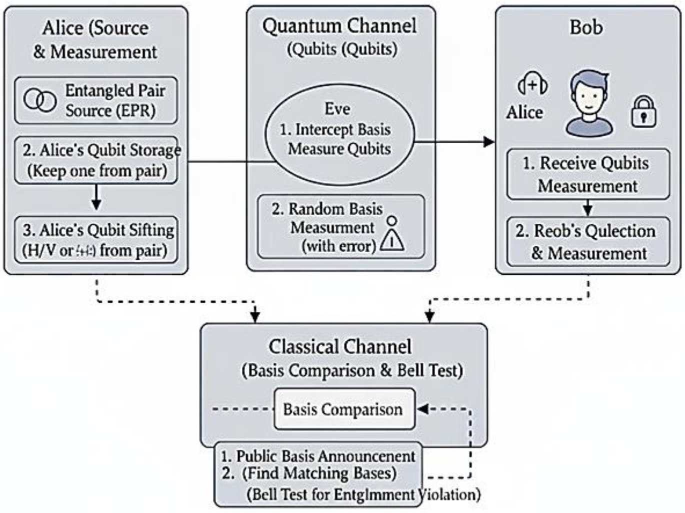
Alice (Source
& Measurement
Entangled Pair Source (EPR)
2. Alice's Qubit Storage (Keep one from pair)
3. Alice's Qubit Sifting (H/V or +/- from pair)
Quantum Channel
(Qubits (Qubits)
Eve
1. Intercept Basis Measure Qubits
2. Random Basis Measurment (with error)
Bob
Alice
1. Receive Qubits Measurement
2. Reob's Qulection & Measurement
Classical Channel
(Basis Comparison & Bell Test)
Basis Comparison
1. Public Basis Announcenent
2. (Find Matching Bases)
(Bell Test for Entglmment Violation)

Figure 3. *Block diagram illustrating QKD transmission using E91 protocol.*

In the first scenario, the source will create 10^5 entangled qubit pairs and send them to Alice and Bob through a quantum channel with a loss rate of 0.1, without Eve's interference. The simulation results are shown in figure 4.

From figure 4, it is observed that under conditions of no eavesdropping and negligible channel loss, the measurement results on the same basis should be perfectly anti-correlated (due to the initial Bell state), so the QBER is close to 0. For the correlation value S, in the absence of eavesdropping, the calculated S value will violate the Bell inequality, i.e., S > 2. Theoretically, it will approach $2\sqrt{2} \approx 2.828$, confirming that the qubits still maintain quantum entanglement and the communication channel is secure. The simulation results are fully consistent with the theoretical calculations in the previous section.

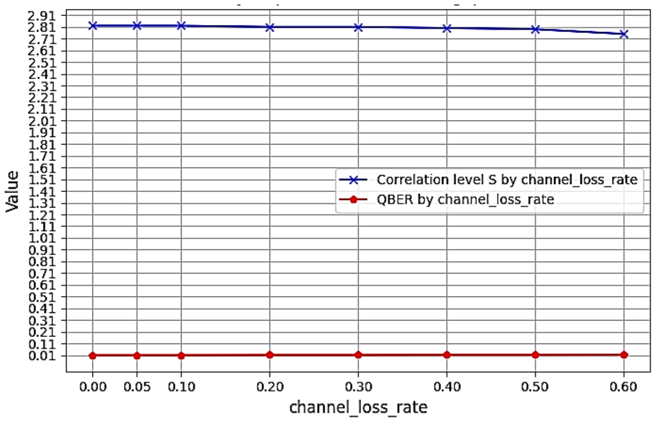

Figure 4. *QBER and S when transmitting via the E91 protocol without eavesdropping.*

In the second scenario, the source will create 10^5 entangled qubit pairs and send them to Alice and Bob through a quantum channel with a loss rate of 0.1. We calculate QBER and the S value as a function of Eve's eavesdropping rate. The simulation results are shown in figure 5.

Figure 5 shows that when Eve intercepts and measures a qubit, the entanglement of that qubit pair is destroyed. Although Eve creates and sends a new qubit to Bob, she cannot recreate the original pair's entanglement. Bob's measurement results become random with respect to Alice's. Therefore, the QBER will increase significantly, approaching 25% when Eve eavesdrops on 100% of the qubits (similar to BB84 in figure 2). Because Eve's eavesdropping action breaks the quantum entanglement, the correlations between Alice's and Bob's measurement results no longer follow the predictions of quantum mechanics but revert to the limits of classical physics. As a result, the S value will drop sharply from ~2.8 to ≤ 2 when the eavesdropping rate is about 25%. The combination of these two factors, a decreasing S and an increasing QBER, is a strong indication of an eavesdropper's presence, demonstrating the superior security of the E91 protocol.

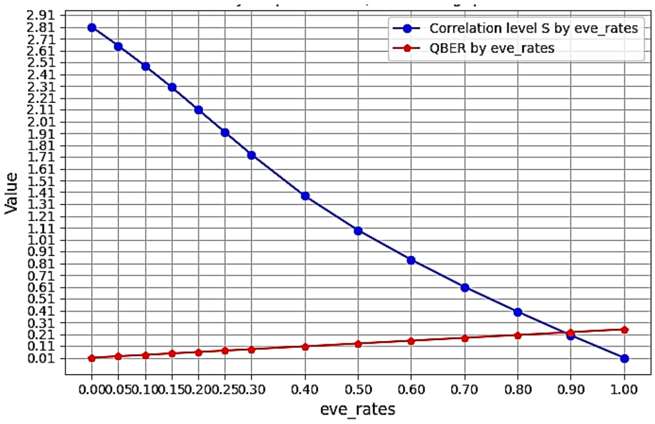

Figure 5. *QBER and S when transmitting via the E91 protocol as a function of eavesdropping rate.*

3.3. Simulating and evaluating a general quantum communication network

The general scenario will simulate a quantum network transmitting a qubit from Alice to Bob through intermediate nodes using quantum repeaters via the entanglement swapping technique and using the advanced quantum protocol of Quantum Teleportation. The quantum network is evaluated through Fidelity (F) from formula (11) as a function of the channel's loss rate and Eve's eavesdropping rate.

The detailed steps for the simulation via the QuNetSim source code are as follows:

- Preparation: Alice creates her own data qubit Ψ_{data};

- Entanglement generation: Alice creates an entangled pair (A1, C1) and sends qubit C1 to node C, which has a quantum repeater. At node C, an entangled pair (C2, B1) is created, and qubit B1 is sent to Bob via Eve;

- Attack Simulation: Eve will intercept qubit B1 on its way to Bob, measure it (destroying the entanglement), and send a junk qubit to Bob;

- Repeater simulation via entanglement swapping: At node C, a Bell state measurement is performed on the two qubits (C1 and C2). This operation connects A1 and B1 to create entanglement between Alice and Bob. The measurement result is then sent to Bob for error correction;

- Teleportation protocol simulation: Alice performs a Bell state measurement on her data qubit |Ψ_data⟩ and A1, and sends this measurement result to Bob;

- Reconstruction: Bob receives the qubit from Eve and the pair of measurement results from Alice and node C, then performs the necessary operations to reconstruct Alice's data qubit;

- Evaluation: The final state of Bob's qubit and Alice's initial data qubit state |Ψ_data⟩ are used to calculate the network's Fidelity F according to formula (11).

The simulation results for the quantum network's fidelity as a function of channel loss rate and Eve's eavesdropping rate in this general scenario are shown in figure 6.

Channel loss does not break the entanglement of qubit pairs; it only causes the loss of qubits. However, using the teleportation protocol via a quantum repeater requires multiple qubits and calculated values to successfully reach the destination in the same run. If just one of them is lost, the entire transmission run fails. Therefore, as the loss rate increases, the probability of a successful teleportation run decreases very quickly, causing Fidelity to drop sharply (the blue line with circular dots in figure 6). In the case of no channel loss and no eavesdropping, the fidelity F = 0.98, which is less than 1 due to background noise and imperfections in the quantum repeater. In this simulation, the repeater divides the long Alice-Bob channel into two shorter segments: Alice-C and C-Bob. It creates entanglement over each of these short segments, then performs "entanglement swapping" to link them, creating a single entangled link between Alice and Bob. Therefore, in this simulation scenario, the repeater significantly increases the number of successful teleportation runs. According to the results in figure 6, the presence of the repeater is the reason why F can reach a high value (e.g., 0.583) even when the channel loss is 30%. Without the repeater, with the same loss level, Fidelity would approach 0.

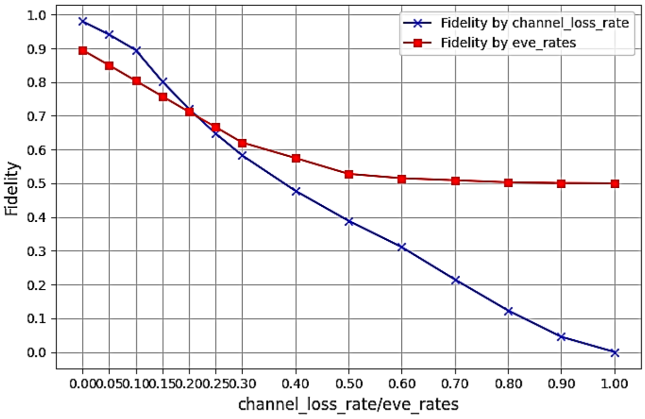

***Figure 6.** Evaluating the fidelity of the quantum network as a function of channel loss and eavesdropping rate.*

When the channel loss is fixed at 0.1 and Eve is not eavesdropping, F reaches its highest level of 0.895 (it cannot reach 1 due to channel loss and background error rates). As Eve's eavesdropping rate increases, more quantum entangled pairs are broken, making the state of the final quantum qubit received at Bob less related to the state of the original qubit at Alice. Consequently, the fidelity F gradually decreases towards the theoretical level of 0.5, where Bob is merely guessing the result randomly.

Thus, this simulation scenario provides a comprehensive evaluation of a complex quantum network with almost all essential components and advanced algorithms. The simulation results also demonstrate the capability of the open-source software QuNetSim in modeling realistic transmission channels and complex protocol chains.

4. CONCLUSIONS

This paper has presented a solution using the open-source software QuNetSim to analyze and evaluate quantum communication networks through simulation. This solution provides readers with a concrete approach to grasp the fundamental concepts, properties, and algorithms in quantum communication networks through simulation. In particular, the general simulation scenario in section 3.3 allows readers to build a custom quantum network, from modeling channel errors and implementing complex protocols like entanglement swapping and teleportation, to simulating eavesdropping attack scenarios to gather information. This is an accessible direction aimed at serving the research and development of a practical hardware-based quantum communication network in the near future.

REFERENCES

[1]. Quantum Open Source Foundation (QOSF). "*Project list*", https://qosf.org/project_list/.

[2]. *"QuNetSim – Quantum Network Simulator",* https://tqsd.github.io/QuNetSim/index.html.

[3]. Dahlberg, Axel, and Stephanie Wehner. "*SimulaQron – A simulator for developing quantum internet software*", Quantum Science and Technology, 4, 1, 015001, (2018).

[4]. Bartlett, Ben. "*A distributed simulation framework for quantum networks and channels*", arXiv preprint arXiv:1808.07047, (2018).

[5]. Quantum Flagship. "*Quantum Repeaters – Quantum Technology*", https://qt.eu/quantum-principles/communication/quantum-repeaters.

[6]. Ekert, Artur K. "*Quantum cryptography based on Bell's theorem*", Physical Review Letters, 67, 6, 661–663, (1991).

[7]. Nielsen, Michael A., and Isaac L. Chuang. "*Quantum Computation and Quantum Information*", Cambridge University Press, (2000). DOI: 10.1017/CBO9780511976667. ISBN 978-0521635035.

[8]. Bennett, C. H., and Brassard, G. "*Quantum cryptography: Public key distribution and coin tossing*", Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India, Vol. 1, 175–179, (1984).

TÓM TẮT

Giải pháp phân tích, đánh giá mạng truyền thông lượng tử thông qua mô phỏng

Bài báo đề xuất một giải pháp toàn diện để phân tích và đánh giá hiệu năng của mạng truyền thông lượng tử thông qua việc sử dụng phần mềm mô phỏng mã nguồn mở QuNetSim. Phương pháp này cung cấp một cách tiếp cận linh hoạt và hiệu quả về chi phí để nghiên cứu các giao thức và tham số mạng trước khi triển khai phần cứng. Nội dung chính của bài báo tập trung vào việc mô hình hóa các yếu tố thực tế như suy hao kênh, nhiễu và các hành vi nghe lén. Nghiên cứu đã thực hiện các kịch bản mô phỏng chi tiết với giao thức BB84 và E91. Đặc biệt, một kịch bản mạng tổng quát, tích hợp bộ lặp lượng tử và viễn tải, đã được phân tích thông qua độ trung thực (Fidelity). Kết quả không chỉ khẳng định vai trò quan trọng của bộ lặp trong việc duy trì kết nối trên khoảng cách xa mà còn định lượng được mức độ suy giảm hiệu năng do suy hao kênh và nghe lén. Kết quả mô phỏng cũng chứng minh QuNetSim là một công cụ mạnh mẽ, giúp các nhà nghiên cứu dễ dàng xây dựng, kiểm tra và tối ưu hóa các mạng lượng tử phức tạp, thúc đẩy quá trình chuyển đổi từ lý thuyết sang thực tiễn.

Từ khóa: Truyền thông lượng tử; BB84; E91; QuNetSim; Mô phỏng.