Secured Quantum Identity Authentication Protocol for Quantum Networks

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: {mmibrahims42, mismail}@tntech.edu

***Abstract*—The emergence of sixth-generation (6G) networks presents a promising paradigm aimed at meeting stringent quality-of-service (QoS) requirements, thereby paving the way for modern applications such as the metaverse. In contrast, the advent of quantum computers poses a significant threat to the security of such networks. However, the quantum Internet signifies a remarkable advancement in communication technology, harnessing the principles of quantum entanglement and superposition to facilitate unparalleled levels of security and efficient computations. Quantum communication can be achieved through the utilization of quantum entanglement. Through the exchange of entangled pairs between two entities, quantum communication becomes feasible, enabled by the process of quantum teleportation. Given the lossy nature of the channels and the exponential decoherence of the transmitted photons, a set of intermediate nodes can serve as quantum repeaters to perform entanglement swapping and directly entangle two distant nodes. Such quantum repeaters may be malicious and by setting up malicious entanglements, intermediate nodes can jeopardize the confidentiality of the quantum information exchanged between the two communication nodes. Hence, this paper proposes a quantum identity authentication protocol that protects quantum networks from malicious entanglements. Unlike the existing protocols, the proposed quantum authentication protocol does not require periodic refreshments of the shared secret keys. Simulation results demonstrate that the proposed protocol can detect malicious entanglements with a 100% probability after an average of 4 authentication rounds. Moreover, the average number of authentication rounds required to detect an attack is reduced by 69% and 76.5% compared with benchmark protocols.**

***Index Terms*—Quantum identity authentication, quantum communications, malicious entanglement, quantum security, quantum Internet, 6G.**

I. Introduction

MODERN applications, such as the metaverse, pose stringent quality-of-service (QoS) requirements in throughput, reliability, and latency. Such requirements cannot be attained by the fifth-generation (5G) networks [1]. Hence, serious efforts are taking place to pave the road toward the sixth-generation (6G) networks. However, the emergence of quantum computers poses a significant threat to the security of existing classical networks. It will necessitate reevaluating security measures since many of the security algorithms currently in use can be easily broken by quantum computers. Shor's algorithm, for example, can efficiently factorize large numbers and solve the discrete logarithm problem, compromising the security of cryptographic algorithms like Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC). In contrast, quantum communications offer unconditional security leveraging the inherent properties of quantum mechanics. Thus, quantum communications promise to enhance the security of 6G networks [2]. In addition, the adoption of quantum communications can improve the attained QoS by further reducing overheads, latency, and congestion, hence, enabling key features of 6G networks [2].

Quantum communications can be enabled via quantum entanglement. By sharing an entangled pair between two parties, quantum communications can be carried out over the classical Internet via quantum teleportation. This eliminates the requirement of having direct quantum channels between every two nodes. To initiate quantum communication, an entangled pair of photons can be generated and transmitted over a quantum channel to communication parties. However, these channels are lossy and the transmitted photons decay exponentially over distance. To overcome this limitation, quantum repeaters can perform entanglement swapping to entangle distant parties. However, the intermediate quantum repeaters may be malicious. By establishing malicious entanglement, an intermediate node would jeopardize the confidentiality of the quantum information exchanged between two parties. This can be achieved by keeping the entangled pair secretly at the intermediate node instead of swapping them out, resulting in a man-in-the-middle (MitM) attack. Since qubits are closed systems until measured, neither party of the legitimate communication nodes can be certain that his/her part of the entangled pair is legitimately entangled with the other party. It is essential to emphasize that malicious entanglement poses a significant threat to the integrity of the exchanged quantum information, particularly when subjected to measurement in the wrong basis by a malicious repeater. Thus, it is necessary to develop an effective authentication protocol that secures quantum communications against malicious entanglements.

A. Related Works and Limitations

The work in [3] proposed a protocol for quantum identity authentication that relies on a shared classical secret key and a single photon. Also, [4], [5] present quantum identity authentication protocols based on the principles of quantum key distribution. In addition, [6] proposes a quantum identity authentication protocol using a cluster state of five qubits. Furthermore, in [7], a protocol is proposed for quantum identity authentication and key agreement by adopting ran-

This work was supported by NSF Award # 2210251.

dom numbers to agree on the session key. Also, in [8], a protocol is introduced for quantum identity authentication by employing non-orthogonal states. Moreover, a semi-quantum identity authentication protocol was proposed in [9] using single-qubit measurement and XOR operations. Additionally, [10], [11] proposed quantum identity authentication protocols based on quantum secure direct communication. Lastly, [12] proposed a quantum identity authentication protocol centered on the utilization of quantum rotation properties and public key cryptography in a bit-oriented approach.

Limitations: Most of the aforementioned quantum authentication protocols rely on quantum channels to transmit authentication qubits between the two communicating parties. Such channels are lossy and transmitted photons will decay over distance, which will reduce the success probability of the authentication process. Also, some protocols may leak information about the shared secret key, and hence, require a periodic refreshment of the shared secret keys. Additionally, existing protocols perform the authentication only at the start of the session, leaving room for potential session hijacking by eavesdroppers after initiation.

B. Contributions

To overcome the existing limitations, the following contributions have been carried out:

- We propose a protocol that establishes authentication between communication parties in quantum networks. The proposed protocol relies on entanglement and reusable shared secret keys. Additionally, the protocol incorporates periodic authentication as a proactive measure to minimize the vulnerability to session hijacking.
- We perform a security analysis of the proposed protocol, which demonstrates that the detection probability of a malicious entanglement increases based on multiple authentication rounds from 50% to reach 100% by the fourth round of the authentication process.
- We simulated the proposed protocol in a quantum network, which provided numerical results that support our security analysis. The simulations were carried out on a quantum network simulator, QuNetSim [13]. The simulation results demonstrate that the proposed protocol significantly enhances security by reducing the average number of required authentication rounds by 69% and 76.5% compared with benchmark protocols.

The rest of this paper is organized as follows. Section II defines the problem of malicious entanglement in quantum networks and presents the proposed quantum identity authentication protocol and provides an illustration example. Section III presents a security analysis of the proposed protocol and discusses the simulation setup and results. Section IV concludes the paper.

II. Problem Definition and Proposed Quantum Authentication Protocol

A. Problem Definition

Consider a quantum network represented as a graph $G = (V, E)$, where $V = \{v_i\}_{i=1}^{N}$ represents a set of N nodes while $E = \{e_{i,j}; v_i, v_j \in V\}$ represents the set of edges connecting the nodes. Consider entangled pairs being already distributed among adjacent nodes. Let node v_i want to send quantum data to a non-adjacent node v_j and there is no direct quantum channel between v_i and v_j. Hence, nodes v_i and v_j communicate via quantum teleportation. Being non-adjacent nodes, there is no entangled pair shared between v_i and v_j. Consider an intermediate node v_k that shares entangled pairs with v_i and v_j such that $e_{i,k} \in E$ and $e_{j,k} \in E$. Then, v_k can perform entanglement swapping to directly entangle v_i and v_j. Given the aforementioned model, this paper aims to provide a protocol that enables v_i and v_j to authenticate each other and ensure that v_k did not perform a malicious entanglement. The proposed protocol works on any number of intermediate nodes and the adoption of a single intermediate node herein is meant only for illustration purposes.

B. Proposed Quantum Authentication Protocol

The proposed authentication protocol assumes that the two end users share a secret key in advance, which can be done using a key management protocol such as quantum key distribution. Following the common terminology, let the end users be called Alice and Bob. Let Alice want to use teleportation to send quantum data to Bob. Through entanglement swapping via intermediate node(s), Alice and Bob can share an entanglement pair. Alice wants to authenticate Bob to ensure that she is sending the quantum information only to Bob and that the intermediate node(s) did not create a malicious entanglement.

1) Steps of the Proposed Protocol: The proposed authentication protocol works as follows:

1) Alice and Bob agree first on three parameters, namely, encoding index, base index, and transfer length. The encoding index is used to determine the initialization of an authentication qubit. The base index is used to determine the encoding and measurement bases of the authentication qubit. The transfer length is used to identify the number of data qubits that will be sent before an authentication qubit is sent. The encoding index and base index $\in \{0, 1\}$ and must be the opposite of each other. For example, if the encoding index is 1, then the base index must be set to 0, and vice versa. For this reason, Alice and Bob do not need to agree on these two bits explicitly, they may agree on one of them and the other one will be set implicitly.
2) Alice and Bob use the transfer length and the shared secret key to calculate the number of data qubits that will be transferred before an authentication qubit is sent. The authentication process is repeated after every R data qubits are transferred where R is dynamic during a communication session between Alice and Bob and

should be recalculated for each authentication round. For example, let K be the shared secret key between Alice and Bob. Let Alice and Bob agree on a transfer length of T. Each of them will select the first T bits from the secret key K and calculate R as their decimal equivalent. Then, Alice will send R data qubits before waiting for an authentication qubit from Bob. Also, Bob will receive R data qubits from Alice before sending an authentication qubit to Alice. Upon the reception of these R qubits, the authentication process starts and after the authentication process is complete, Alice and Bob recalculate R from the next T bits of the secret key K. Hence, the number of data qubits sent before the authentication process changes after every authentication.

3) Based on R, Alice keeps sending R data qubits to Bob.
4) Bob keeps receiving R data qubits from Alice.
5) Bob prepares an authentication qubit as follows:
   a) Bob sequentially chooses pairs of bits from the secret key, denoting the i-th two bits as the focal point. In the initial authentication round, this selection encompasses the first and second bits. Subsequently, in each successive round, the third and fourth bits take center stage, followed by the subsequent pairs in a similar manner. Notably, the first bit retains an index of 0, while the second bit maintains an index of 1 throughout each authentication round.
   b) Bob uses the encoding index and the base index to identify the initialization of the authentication qubit (encoding bit) and the encoding base (base bit) from the two bits selected at step (5a).
   c) Bob creates an authentication qubit based on the identified values at step (5b). If the encoding bit is 0, the authentication qubit is initialized to $|0\rangle$, otherwise, it is initialized to $|1\rangle$. If the base bit is 0, the authentication qubit is encoded in the Z-bases, otherwise, it is encoded in the X-bases. Hence, the authentication qubit should be in one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$.
   d) Bob teleports the authentication qubit to Alice.
6) Alice receives the authentication qubit from Bob and decodes it as follows:
   a) Alice selects the i-th two bits from the secret key.
   b) Alice uses the encoding and the base indices to identify the measurement value and the measurement base from the two bits selected at step (6a).
   c) Alice measures the authentication qubit based on the measurement base extracted at step (6b), then, compares the result to the measurement value extracted at step (6b). If they are not matched, then Bob's authentication has failed and Alice should terminate the session immediately.
7) Alice and Bob calculate new R and repeat the process from step (3).
8) If Bob wants to authenticate Alice, the same process is carried out in a reversed manner. But this means that Alice and Bob will sacrifice another entangled pair to do the reverse authentication.

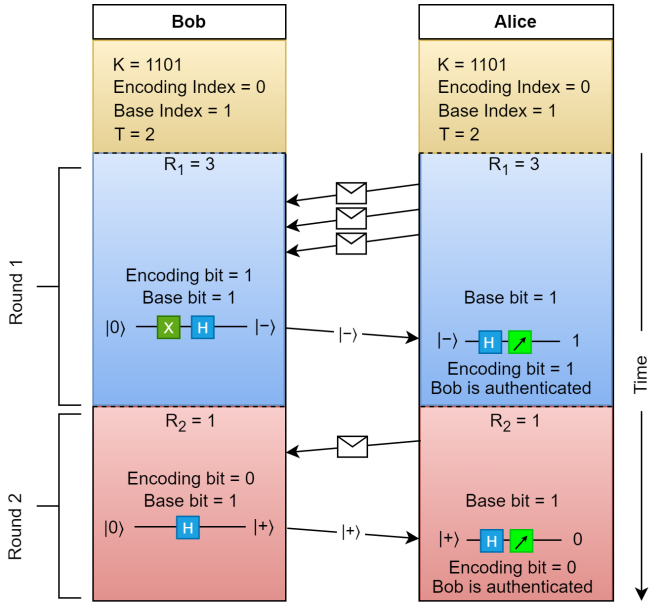

Fig. 1. Illustration example of the proposed represented as timeline diagram.

2) Illustrating Example: To further explain the proposed protocol, the following example illustrates the first authentication round: Let Alice and Bob share secret key $K = 1101$ and agreed on an encoding index 0, base index 1, and transfer length $T = 2$. Fig. 1 illustrates the steps of the proposed protocol as a timeline diagram.

Step-1: Alice and Bob pick the first two bits from the key 11 and convert them to decimal, which results in 3. Alice and Bob calculate $R_1 = 3$.

Step-2: Based on R_1, Alice teleports 3 data qubits to Bob before starting the authentication process. Also, Bob receives 3 data qubits from Alice before starting the authentication.

Step-3: The initial value and encoding base of the authentication qubit are extracted by selecting the first two bits from the key, where the encoding index is the first bit, and the base index is the second bit, and the bits are 11. Bob then initializes the authentication qubit to 1 in the X-bases using an X-gate followed by an H-gate, resulting in $|-\rangle$. Finally, Bob teleports the authentication qubit $|-\rangle$ to Alice.

Step-4: Alice selects the first two bits from the key. The first bit is used as the encoding index, and the second bit is used as the base index. Alice measures the authentication qubit in the X-base and compares the result with the expected measurement value extracted from the key. If they match, authentication continues, and if not, Alice terminates the session immediately as this indicates the presence of an unauthorized party.

Repeat: If Alice successfully authenticates Bob, they repeat the same steps until the session ends. In the second round, $R_2 = 1$. Hence, Alice sends 1 qubit data to Bob before Bob starts to authenticate himself. When Bob authenticates himself, the authentication qubit will be $|+\rangle$.

III. Security Analysis, Simulation Results, and Discussion

A. Security Analysis

Assume Alice wants to send quantum data to Bob and an intermediate node (Eve) attempts to perform malicious entanglement. In this case, Alice and Bob are not directly entangled which means that Eve shares an entanglement pair with Bob and an entanglement pair with Alice. Alice and Bob share a secret key and Eve does not know the key. Suppose only Alice wants to authenticate Bob which is sufficient in some cases. Alice and Bob start the authentication process after a few transmitted qubits. Bob will prepare the authentication qubit and teleport it to Alice. In the malicious entanglement case, Eve will receive the qubit instead. Because Eve does not know the key, she will never know that this is an authentication qubit and will measure it. The arbitrary measurement performed by Eve on the authentication qubit will enforce the qubit to collapse in one of two possible states $|0\rangle$ or $|1\rangle$ and then Eve sends the qubit to Alice. The quantum information in the qubit prepared by Bob has been destroyed and Alice will detect the attack with a probability of 50% after the first authentication round. This is because the authentication qubit has the chance to collapse to the correct value with a probability of 50%. After the second, third, and fourth authentication rounds, Eve will be detected with a probability of 75%, 87.5%, and 93.75%, respectively. Within 7 authentication rounds, Eve will be detected with a probability of 99.2%. Also, Eve cannot impersonate Bob by constructing an authentication qubit because she does not know the key. So, she cannot know the initialization and encoding bases. Additionally, she does not know when Alice and Bob will perform the authentication because Alice and Bob do the authentication dynamically and secretly. It is worth noting that the same analysis remains valid in scenarios where multiple repeaters are malicious and performing malicious entanglement. This is because once the first malicious repeater measures the quantum state, it collapses to either $|0\rangle$ or $|1\rangle$, rendering subsequent measurements ineffective as the initial measurement already destroys the quantum information. Consequently, the protocol maintains its resilience against collaborative attacks by multiple malicious repeaters.

The transfer length controls the amount of data transferred before each authentication. For example, a transfer length of 2 can allow a maximum of 3 qubits to be transferred before each authentication. A transfer length of 4 can allow a maximum of 15 qubits to be transferred before each authentication process. On the one hand, if Alice and Bob transfer sensitive data, they may decrease the transfer length to do more authentication rounds and increase the probability of detecting Eve before transmitting much data. On the other hand, Alice and Bob can increase the transfer length for higher throughput with fewer overheads if they are not transferring sensitive data.

Lastly, it is important to highlight that within their quantum communication setup, Alice and Bob do not rely on classical communication beyond the essential exchange of two classical bits needed for the recovery of teleported quantum states. This classical channel does not necessitate stringent security measures and remains unaffected by compromise.

B. Simulation Results

This paper used QuNetSim [13] to simulate the proposed protocol and evaluate its performance. To test the security level of the proposed protocol, a malicious entanglement attack was simulated where Alice wants to communicate with Bob and there is a malicious node (Eve) performing a malicious entanglement attack between Alice and Bob. Alice shares an entangled pair with Eve, and Eve shares an entangled pair with Bob. It is supposed that Eve applies entanglement swapping to entangle Alice and Bob directly, but in this malicious scenario, Eve will not perform the entanglement swapping, which results in a MitM attack. The simulation scenario is tested for transfer lengths $T = \{1, 2, 3, 4, 5\}$, which means that the maximum number of data qubits transferred between two authentication rounds are $1, 3, 7, 15, 31$, respectively. For each transfer length, the simulation scenario is repeated 200 times attempting to send 150 data qubits from Alice to Bob. In each transfer, Eve receives a qubit from Alice, measures it in a random base, and then teleports it to Bob.

The success rate of the protocol is measured as shown in Fig. 2 where the proposed protocol can detect the attack with a probability of 100% for the transfer lengths $1, 2$, and 3 while it degrades to 99.5% and 96.5% for the transfer lengths 4 and 5, respectively. This is because the number of authentication rounds performed is not enough compared with the amount of transferred data. The average number of authentication rounds required to detect an attack has been measured for each case as shown in Fig. 3. The simulation results show that the proposed protocol is able to detect an attack within 4 authentication rounds on average. Although the security analysis presented in section III-A calculates that an eavesdropper would be detected within 7 rounds with a probability of 99.2%, the simulation results showed that an eavesdropper can be detected with a probability of 100% within 4 rounds. The security analysis focuses on calculating the worst-case scenario of detecting eavesdropping, while the simulation results calculate the average number of authentication rounds required to detect an attack within 200 trials.

The average data leakage has been measured for each case and shown in Fig. 4. The data leakage is the number of qubits transmitted from Alice to Bob before detecting the presence of Eve. The results presented in Fig. 4 clearly demonstrate that the average data leakage increases as the transfer length increases. The underlying reason for this phenomenon is that as the transfer length increases, more qubits are transferred between two authentication rounds on average, providing Eve with more opportunities to gain information before being detected. Given the clear relationship between transfer length and data leakage demonstrated in Fig. 4, it is important for Alice and Bob to carefully consider the confidentiality level of the data they are transferring when selecting an appropriate transfer length. If the data is highly sensitive, Alice and Bob

should prioritize security over speed and choose a shorter transfer length. This will allow for more frequent authentication rounds, increasing the probability of detecting Eve before she can intercept and gather a significant amount of data. On the other hand, if the data is less sensitive, Alice and Bob may be able to afford a longer transfer length for faster communication. Ultimately, the decision of transfer length should be based on a careful balance between the confidentiality level of the data being transferred and the desired communication speed. By taking a thoughtful and strategic approach, Alice and Bob can ensure the highest level of security and protection for their data. The data leakage can lead to data integrity loss. Data integrity loss refers to the situation where the integrity or accuracy of data is compromised or altered, leading to inaccuracies, errors, or unauthorized modifications in the stored or transmitted data. It is essential to note that the data integrity loss significantly depends on the type of quantum data being exchanged. Without knowing the specific type of quantum data involved, providing accurate values for data integrity loss could be challenging. For instance, in scenarios where unknown quantum states are delivered and utilized without measurements, such as in distributed quantum computing, where qubits control another target qubit, the data integrity loss in this case is hard to quantify. This is because of the infinite number of quantum states a single qubit can represent if it exists in superposition. However, if the exchanged data involves classical data encoded as qubits, the integrity loss might be around 50% of the data leakage. This occurs because the malicious repeater may measure the qubits in the wrong basis approximately 50% of the time.

To assess the practicality of using the proposed quantum authentication protocol, a simulation was conducted to measure the communication overhead of the authentication process. The communication overhead is defined as the ratio of the number of authentication qubits involved in the communication process to the number of data qubits. As shown in Fig. 5, the communication overhead of the proposed protocol is 64%, 37%, 20%, 10%, and 4% for transfer lengths 1, 2, 3, 4, and 5, respectively. These results demonstrate that while there is some overhead associated with using the proposed quantum authentication protocol, it is relatively small for reasonable transfer lengths. Therefore, the proposed protocol can be considered a viable and practical solution for secure communication between two parties. It is worth noting that the proposed protocol is scalable to large networks. Authentication is exclusively conducted between pairs of communication parties, allowing the protocol to seamlessly accommodate additional nodes without introducing complexity. Furthermore, the protocol's design minimizes the need for classical communication, with only two classical bits required for the recovery of teleported quantum states. This ensures that no additional traffic is introduced over the network, making the protocol efficient and practical for large networks.

The number of qubits that can be transmitted by a single use of the shared secret key depends on the transfer length. For example, if the shared secret key is 1024 bits long and

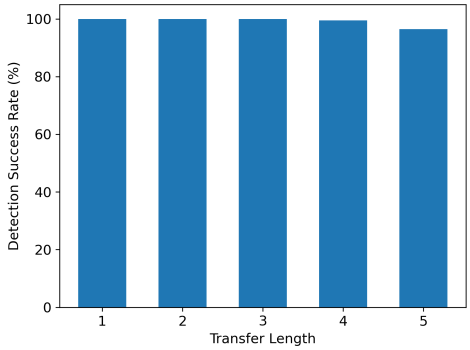

Fig. 2. The success rate of the proposed protocol to detect a malicious entanglement attack, using transfer lengths of $1, 2, 3, 4$, and 5.

the transfer length is 2, then the key can support up to 512 authentication rounds. During each round, up to 3 qubits of data can be sent, but on average only 1.5 qubits are sent. Thus, the total number of qubits that can be sent by a single use of the 1024-length key is 768 qubits on average. If the transfer length is 3, then the same key can support up to 341 authentication rounds. During each round, up to 7 qubits of data can be sent, but on average only 3.5 qubits are sent. Thus, the total number of qubits that can be sent through a single use of the shared key is 1193 qubits on average. Equation (1) can be used to calculate the average number q of qubits that can be transmitted using a transfer length T and a single use of a shared secret key with length L

$$q = \lfloor \frac{2^T - 1}{2} \times \frac{L}{T} \rfloor. \tag{1}$$

However, if the shared secret key is used up, the two parties involved in the communication can start the process again from the first bit. Therefore, the number of qubits that can be sent is multiplied by the number of times the key is used. It is important to note that the shared secret key is highly reusable, as it does not reveal any information about the authentication process during transmission. This allows for a secure, covert authentication process that outside parties cannot detect. Because qubits are closed systems, it is impossible for anyone other than the communication parties to differentiate between the data qubit and the authentication qubit. Also, both the encoding bit and the base bit are fully secure, no one can determine the value encoded into the qubit or the encoding base used even if the authentication qubit is captured.

Finally, the proposed protocol has been compared to quantum authentication protocols proposed in [3] and [9], focusing on the average number of authentication rounds required to detect an attack. The proposed protocol significantly reduces the average number of authentication rounds needed to detect an attack to 4 as shown in Table I. This represents a notable improvement of 69% and 76.5% compared to the protocols introduced in [3] and [9], respectively. This improvement is attributed to the effective utilization of the shared key, eliminating the need for classical communication beyond the two classical bits required to recover the teleported quantum states. It is worth noting that maintaining confidentiality for these two

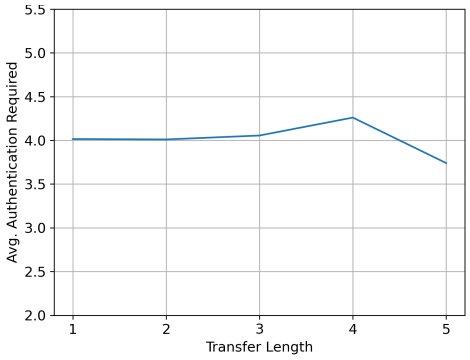

Fig. 3. The average number of authentication rounds required for the proposed protocol to detect an attack, using transfer lengths of $1, 2, 3, 4$, and 5.

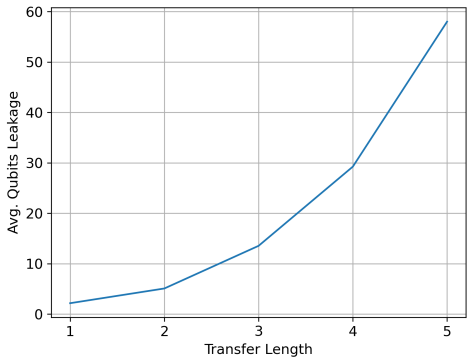

Fig. 4. The average data leakage before detecting an attack and terminating the session, using transfer lengths of $1, 2, 3, 4$, and 5.

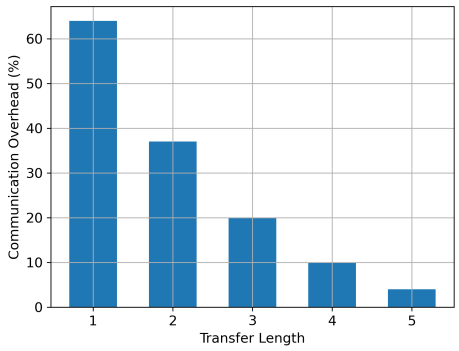

Fig. 5. The average communication overhead of the proposed authentication protocol using transfer lengths of $1, 2, 3, 4$, and 5.

classical bits is unnecessary, and intercepting them does not affect the security of the protocol. Moreover, the proposed protocol introduces periodic authentication, enhancing the security of communication sessions between communication parties. This stands in contrast to benchmark protocols, which only perform authentication at the start of the communication session. In such cases, eavesdroppers could potentially hijack the session after initiation. Our periodic authentication significantly contributes to a more secure communication environment, mitigating such vulnerabilities.

IV. Conclusion

This paper proposes a quantum identity authentication protocol to detect malicious entanglement over quantum networks. To validate the effectiveness of the proposed protocol, comprehensive simulations have been conducted using the QuNetSim simulator. The simulation results show that the proposed algorithm can detect malicious entanglement within 4 authentication rounds on average. The simulation results also showed that the proposed protocol has a minimal communication overhead when a reasonable transfer length is used. Furthermore, the proposed protocol has been compared with two benchmarks, revealing a reduction by 69% and 76.5% in the average authentication rounds required to detect an attack.

In future work, we will conduct a comprehensive investigation into the effects of noise on the proposed authentication protocol. Also, more attack scenarios will be studied and a security analysis will be provided for each attack scenario.

TABLE I
Comparing the proposed protocol with benchmarks.

Protocol	Avg. authentication rounds	Detection probability
[3]	13	99.9%
[9]	17	100%
Our protocol	4	100%

References

[1] L. U. Khan, I. Yaqoob, M. Imran, Z. Han, and C. S. Hong, "6G wireless systems: A vision, architectural elements, and future directions," *IEEE Access*, vol. 8, pp. 147 029–147 044, 2020.

[2] C. Wang and A. Rahman, "Quantum-enabled 6G wireless networks: Opportunities and challenges," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 58–69, 2022.

[3] C. h. Hong, J. Heo, J. G. Jang, and D. Kwon, "Quantum identity authentication with single photon," *Quantum Information Processing*, vol. 16, no. 10, p. 236, Aug 2017.

[4] B. Liu *et al.*, "Quantum identity authentication in the counterfactual quantum key distribution protocol," *Entropy*, vol. 21, no. 5, 2019.

[5] Z. Chen, K. Zhou, and Q. Liao, "Quantum identity authentication scheme of vehicular ad-hoc networks," *International Journal of Theoretical Physics*, vol. 58, no. 1, pp. 40–57, Jan 2019.

[6] X.-y. Zheng and Y.-x. Long, "Controlled quantum secure direct communication with authentication protocol based on five-particle cluster state and classical xor operation," *Quantum Information Processing*, vol. 18, no. 5, p. 129, Mar 2019.

[7] H. Zhu, L. Wang, and Y. Zhang, "An efficient quantum identity authentication key agreement protocol without entanglement," *Quantum Information Processing*, vol. 19, no. 10, p. 381, Oct 2020.

[8] A. Babu and N. Shanthi, "Quantum identity authentication using non-orthogonal state encoding," in *2021 2nd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS)*, 2021, pp. 334–337.

[9] S. Jiang, R.-G. Zhou, and W. Hu, "Semi-quantum mutual identity authentication using bell states," *International Journal of Theoretical Physics*, vol. 60, no. 9, pp. 3353–3362, Sep 2021.

[10] A. Dutta and A. Pathak, "Controlled secure direct quantum communication inspired scheme for quantum identity authentication," *Quantum Information Processing*, vol. 22, no. 1, p. 13, Dec 2022.

[11] B. D. Rao and R. Jayaraman, "A novel quantum identity authentication protocol without entanglement and preserving pre-shared key information," *Quantum Information Processing*, vol. 22, no. 2, p. 92, Jan 2023.

[12] G. Chen, Y. Wang, L. Jian, Y. Zhou, and S. Liu, "Quantum identity authentication based on the extension of quantum rotation," *EPJ Quantum Technology*, vol. 10, no. 1, p. 11, Apr 2023.

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