Quantum Network Security: A Quantum Firewall Approach

Shahad A. Hussein[1], Suadad S. Mahdi[1] and Alharith A. Abdullah[1]

Abstract—**The increasing prominence of quantum networks has necessitated the exploration of their vulnerabilities and the development of effective countermeasures. This paper investigates the potential threats faced by quantum networks, particularly focusing on the exploitation of quantum TCP-three-way handshake connections. To mitigate these attacks, a novel approach involving the implementation of a quantum firewall is proposed. The paper emphasizes that the security of quantum networks is primarily reliant on pre-established agreements for creating quantum entanglement among devices, which inherently limits external attacks. However, it highlights the adverse impact of quantum assaults on network availability due to the consumption of quantum bits required for establishing connections. By leveraging unique node identification and coherence time of quantum memory, the proposed quantum firewall effectively mitigates the effects of attacks while ensuring network availability. Through this security strategy, the paper demonstrates the robustness of the quantum firewall in safeguarding the integrity and operation of quantum networks against potential threats.**

Index Terms—**Quantum Internet, Quantum Repeater, Quantum Attack, Quantum Firewall**

I. INTRODUCTION

The rapid evolution of quantum technology has led to the emergence of quantum networks as a vital component of modern communication systems [1]. As these networks become increasingly complex and critical, ensuring their security against potential threats has become of paramount importance. Consequently, recent research has dedicated significant attention to examining the security aspects of quantum networks, as evidenced by numerous articles in the field.

Quantum networks offer new avenues for secure and efficient information transfer by leveraging the principles of quantum mechanics [2]. However, these networks also introduce unique challenges and vulnerabilities that must be thoroughly understood and effectively addressed. Researchers have directed their efforts toward investigating the security implications of quantum networks, exploring potential threats, and devising strategies to mitigate them.

The exploration of security in quantum networks spans various dimensions, encompassing the protection of quantum communication protocols and the resilience of network infrastructure [3]. Researchers have developed novel techniques and frameworks to ensure the confidentiality, integrity, and availability of quantum information transmitted over these networks, aiming to establish a robust foundation for their secure operation.

In the context of this research, one notable paper [4] introduces a quantum intrusion detection system (QIDS) that combines conventional and quantum approaches to effectively protect systems against sophisticated attacks. The QIDS enhances accuracy, precision, and reduces false positives, with evaluations conducted using Distributed Denial of Service (DDoS) assaults generated by Mirai botnets.

Despite advancements in quantum technology, the practicality of a quantum internet is limited due to the constraint of point-to-point qubit transmission. Overcoming this limitation necessitates the implementation of quantum routers. Notably, studies described in [5][6] present quantum router designs that leverage teleportation and protocols for managing entangled pairs, with validation performed using quantum simulators.

Furthermore, [7] focuses on attacks targeting quantum repeaters, which are akin to traditional Internet routers, evaluating their vulnerabilities in terms of secrecy, integrity, and availability. The authors develop a framework for exploring network-wide vulnerabilities, emphasizing the role of classical computing and networking aspects in addressing the overall security concerns of quantum networks.

In [8], classical network theory and graph theory are employed to address security and key management challenges in quantum networks. The proposed communication architecture prioritizes high security by reducing the number of intermediary nodes. Additionally, key management and data scheduling algorithms enhance data transmission efficiency.

The paper outlined in [9] explores denial of service (DoS) attacks against actual quantum key distribution (QKD) equipment, where attackers deplete the QKD key reserves of the Key Management System (KMS). The authors propose safety measures to mitigate such attacks and underscore the significance of integrating QKD into standard telecommunications networks for ensuring communication security. They also emphasize the importance of treating QKD keys as valuable and scarce resources.

This paper delves into the security aspects of quantum networks, specifically focusing on the vulnerabilities associated with quantum TCP-three-way handshake connections

Submitted on 2024.11.22
[1] University of Babylon, Babil, Iraq;
(E-mail: {shahad.alshamary, suadadsafaa, alharith}@uobabylon.edu.iq)

DOI: 10.36244/ICJ.2025.1.6

[10][11][12]. It also elucidates a strategy for attacking quantum networks, shedding light on potential risks associated with the utilization of quantum communication protocols. The disruption caused by attackers exploiting quantum TCP-three-way handshake connections raises significant concerns. In response to this identified weakness, our research proposes and implements a novel solution: a quantum firewall.

Thus, the primary objectives of this paper are twofold: first, to uncover weaknesses in quantum networks that can be exploited through organized assaults, and second, to establish a quantum firewall as a proactive defense mechanism against such threats. Our findings highlight the importance of establishing quantum entanglement between devices and emphasize the vital role of pre-established agreements in safeguarding against external attacks [13].

By addressing these objectives, our paper contributes to the overall understanding and enhancement of quantum network security. We aim to uncover vulnerabilities, propose effective countermeasures, and provide insights for the development of secure and resilient quantum networks in an increasingly interconnected world.

II. THE PRELIMINARIES

A. The Quantum Network

Quantum networks represent an innovation in information processing and communication, utilizing quantum mechanics principles to provide capabilities previously unavailable to conventional networks [14]. Before delving into the details of this research and innovating a quantum firewall, it is significant to understand some essential concepts in the field of quantum networks which include the following:

a) Quantum bits, or qubits, differ considerably from classical bits, the qubits exist in multiple states at the same time due to the property of quantum superposition [15]. This characteristic significantly improves quantum networks' information processing capability.

Quantum entanglement is the basic idea behind quantum networks. Which is phenomenon shows the existence of a unique relationship between quantum particles. This principle was proposed by the scientist Einstein, who pointed out the existence of a shared state of two particles. Where the two particles are affected together, even if the action occurs on only one of the them. In addition, this type of quantum correlation holds regardless of the distance between the particles [1][13]. Moreover because of this quantum interconnection, measuring the state of one particle make it possible to obtain the state of the other also. Thus, leads to breaking the entangled system. Therefore, quantum entanglement has become a major resource for secure quantum communication [14].

Although the quantum internet depends on the entanglement swapping of entangled pairs of qubits (experiments showed that there are four pairs of entangled qubits, and each pair has two qubits called Bell states that can be represented in equations 1, 2, 3 and 4). The pairs resulting from entanglement swapping cannot be in independent states. In other words, the pairs resulting from this process are in an entangled state. In addition, the state of one pair cannot be separated into two independent states. Moreover, it depends on the measurement result. This is due to quantum mechanics, which is subject to the principle of probability. However, the state of each entangled pair is known after the completion of the quantum swap. At last, the behavior of quantum networks is affected by this concept, which is essential to several aspects such as the Quantum Key Distribution (QKD) and repeaters [16][17].

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (1)$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (2)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (3)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (4)$$

c) Quantum information is sensitive as well as vulnerable to decoherence [18]. Quantum memories (QM), also known as quantum optical memories, are essential components for storing and retrieving quantum states. They are considered the main component responsible for storing a large amount of quantum information in quantum bits of both entangled and non-entangled types, which represent the core of communication in the quantum internet. Furthermore, the lifetime of quantum memories is very short as it depends on the coherence time, which represents the amount of time a quantum system maintains its precise superposition and is crucial for quantum networks to function properly [19], as well as the quantum measuring device such as Bell State Measurement (BSM), and entanglement generator are considered components of quantum memories. Quantum memories have different types, the most famous of which are nitrogen vacuum centers (NV) QM and trapped ionic QM.

d) Quantum nodes represent the heart of the quantum internet. Where, long-range communications between the sender and the receiver are carried out through these nodes. This is done by the entanglement swapping between the quantum memories present in these nodes. Although quantum nodes are subject to quantum laws quantum laws in the process of transferring information, they use the classical internet to exchange control messages between the nodes of the quantum network [12]. In addition, these quantum nodes communicate with each other through quantum and classical channels, like optical fibers or free space[1].

e) Quantum Key Distribution (QKD) referred to the methods employ by quantum network for secure communication. QKD uses quantum features to allow two parties to create a secret key that is secure against attacks like eavesdropping [20] [21].

f) Quantum teleportation a property distinguishing quantum networks that enables the transport of quantum information from one point to another without any physical movement of particles [22]. This mechanism influences the scalability and long-distance communication capacities of quantum networks [23].

All of these concepts establish a structure for understanding the details and constraints of using quantum physics to effectively and securely communicate information.

B. Quantum Transmission Control Protocol (QTCP)

QTCP is the quantum version of TCP, allowing nodes in quantum networks to communicate in a reliable and orderly

manner by using quantum three-way handshake process as shown Fig.1 [12]. QTCP uses qubits, allowing several states to exist at the same time by leveraging quantum superposition principles. This distinguishing feature enables more efficient and complicated transfer of data between quantum nodes, hence improving the overall performance of quantum communication systems.

Furthermore, QTCP uses quantum entanglement to build reliable links between nodes, using the inherent correlations between entangled particles to enable instantaneous and secure data transfer. Despite this, QTCP poses new security issues, such as the vulnerability to eavesdropping and the possibility of quantum state modification during transmission [12].

Additionally, to address these weaknesses and preserve the integrity and secrecy of quantum communication, some security solutions including are employed like intrusion prevention, detection systems and firewall. From point of the quantum view the firewall uses quantum mechanics concepts to create strong defensive mechanisms against possible attacks on Quantum TCP connections, hence protecting the integrity and security of quantum networks.

Understanding the complexities of Quantum TCP is critical for understanding the unique difficulties and solutions in quantum network security, emphasizing the need for more research and development in this quickly expanding sector.

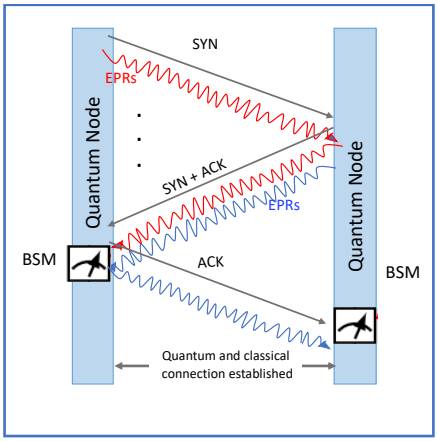

Fig. 1. The Three-way Handshek Process of QTCP [10]

C. *Distributed Denial of Service (DDoS) attacks*

In traditional networks, overloading a target with a flood of traffic from several sources is known as DDoS, which leaves services unreachable [19]. On the other hand, the introduction of Quantum DDoS in the quantum computing age has created a new danger scenario. Quantum DDoS takes advantage of quantum mechanics principles to impair the availability and operation of quantum networks, bringing the classic DDoS idea into the quantum domain. The new attack presents distinct obstacles that require detailed knowledge to design effective responses.

Quantum networks, although providing unparalleled benefits, can pose new vulnerabilities. These weaknesses are exploited by quantum DDoS attacks, which target the quantum channels and memory that contain the fundamental units of quantum information (qubits) as well as required for communication between quantum nodes, where the qubits and channels are attractive targets for attackers looking to disrupt network functioning.

Additionally, these attacks impair the coherence required to create and suffer quantum connections inside the network. Each attacking node adds to the decline of quantum channels, causing a cascade effect that compromises the overall availability and dependability of the quantum network.

Furthermore, unlike conventional networks, where external sources might launch DDoS attacks, quantum networks rely on previous agreements to achieve quantum entanglement between devices. Thus, Quantum DDoS attacks cannot come from external sources.

D. *Firewall Concept*

Before getting into the details of the proposed Quantum Firewall concept, it's important to have an understanding of the general idea of a firewall within the area of cyber security in traditional computing. A firewall is a key network security hardware or software that monitors, filters, and controls incoming and outgoing network traffic based on established security rules. It serves as a firewall between a trusted internal network and untrustworthy external networks, such as the Internet, thereby limiting unwanted access and possible cyber risks [24].

Firewalls are classified into various varieties, each with its own set of features and processes for detection and managing network traffic [23]. Packet-filtering firewalls, for example, Proxy firewalls, and another form, stateful inspection firewalls, also known as dynamic packet filtering, each of which is used depending on the security requirements of the network in which it is used. where the security policies that implement by each type of firewall specify how they should handle various forms of network traffic, enforce access controls and prevent unwanted activity. Furthermore, modern firewalls frequently include intrusion prevention and detection technologies to help identify and respond to possible security threats [24].

Understanding the fundamental ideas of firewalls in classical computing gives an ideal starting point for investigating novel methods of network security, including its use in protecting networks in emerging quantum computing such as the quantum firewall illustrated in Fig 2.

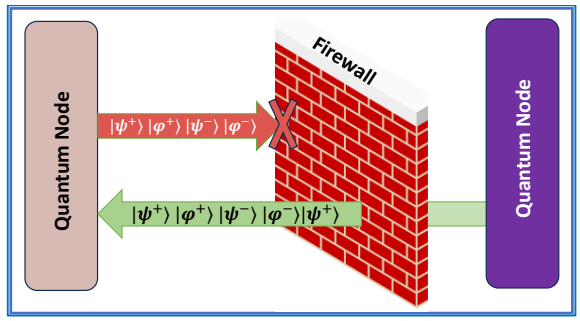

Fig. 2. The Quantum Firewall Concept

III. PROPOSED MECHANISM

The flow work of proposed mechanism outlines a comprehensive system designed to enhance efficiency and security as shown in Fig.3

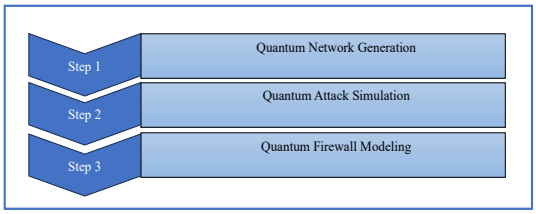

Fig. 3. The Flow Work of the Proposed System

A. Step1: Quantum Network Generation

The Python programming language v3.9, PyCharm Community 2021.3 environment, and a Mac operating system with the Apple M1 processor and 8GB of memory were used to construct the quantum network. The proposed quantum network comprises multiple nodes, each equipped with a quantum memory that has a limited capacity for storing quantum bits. The following factors were considered:

- The Q-network is composed of N nodes, Where the attack-nodes n are chosen according to the equation 5

$$n = round\ (\tfrac{1}{4}\ N) \qquad (5)$$

- The quantum memory has maximum capacity (Max_Cap) ranges from 3 to 9 qubits.
- The nodes are interconnected in a mesh network architecture.
- It is not possible for the quantum channels/links to share a single qubit. A visual representation of the network can be seen in Fig. 4.
- Each node has unique id as (1,2,3 .....n)

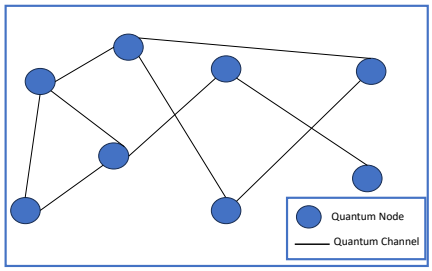

Fig. 4. The Proposed Netwok Architecture

B. Step2: Quantum Attack Simulation

The QTCP protocol's three-way handshake process is vulnerable to a quantum attack that exploits this weakness. The attack involves using EPR to establish Quantum SYN Flooding, as described in the following:

- Each fake node first calculates the number of connections with each neighbor, i.e., check the unbounded channels UC.
- The fake node then prepares a number of local entangled states EPRs in order to begin the quantum three-way handshake process (Connection establishment) according to equation 6

$$EPR_s = UC * Max\_Cap \qquad (6)$$

Moreover, the prepared states are formed as in equation 7 :

$$|\psi^+\rangle_{AiBi}, |\psi^-\rangle_{AiBi}, |\varphi^+\rangle_{AiBi}, |\varphi^-\rangle_{AiBi} \qquad (7)$$

Where the state is represented in two digits that are the node IDs A *and* B and i is an integer from 0 onwards.

- At this stage, the deceptive nodes send qTCP packets (quantum synchronization -qSYN- request) to all nearby nodes via all available channels, in order to occupy the entire channel. Additionally, consists of the sending node's identifier and the second qubit of the entangled bits generated, which represents a qubit stored in the quantum memory of the neighboring node. Nonetheless, the entanglement process remains unfinished as the deceptive node does not complete the three-way handshake process, resulting in half-open communications. the qSYN request is shown in Fig. 5.

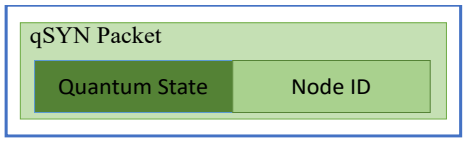

Fig. 5. The Quantum Synchronization Request Packet

- After the coherence time expires, the deceptive nodes resend the qSYN packet again (making qSYN flood attack) as it illustrated in Fig. 6, and it remains in this state repeatedly, consuming the quantum memory of neighboring nodes in addition to the channels between each pair of nodes.

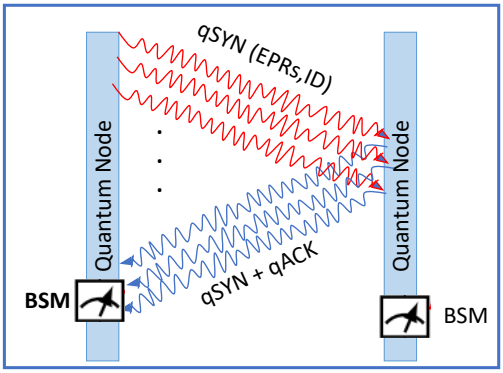

Fig. 6. The Quantum Synchronization Flooding

The flowchart of the quantum-TCP attack is displayed in Fig. 7.

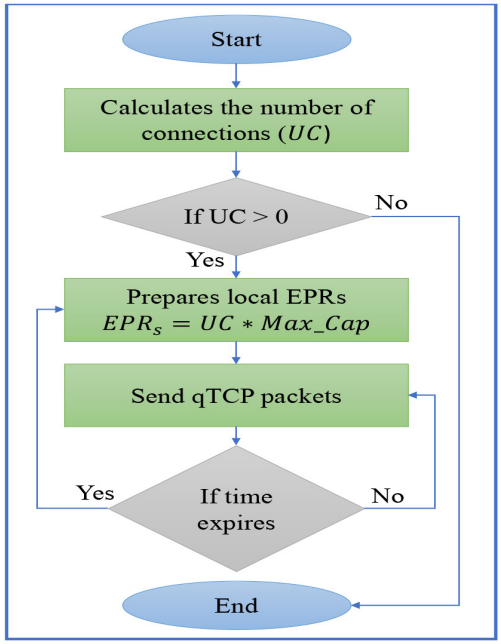

Fig. 7. The Quantum-TCP attack Flowchart

C. Step3: Quantum Firewall Modeling

The quantum firewall is software that runs on all quantum nodes in the network to protect them from quantum communications that may threaten the security and availability of the network. The proposed firewall works as follows:

- We assume that the firewall contains a database (DB) in which the received quantum packet information is recorded.
- The firewall records the time the quantum packet reaches the recipient.
- After that, it extracts the identifier from the quantum packet by performing the quantum measurement process, without sending back the measurement result during which the formation of the quantum link is completed.
- The extracted ID is compared with the IDs stored in the database. If there are no records for this packet, the firewall allows the quantum communication process to complete by performing the measurement process. However, if the number of requests (RC) is more than the threshold specified after the coherence time expires for the quantum memories (determined by comparing the information extracted from the quantum packet and the records belonging to the firewall), then the firewall blocks this node and all incoming requests as the flowchart in Fig. 8 illustrates.

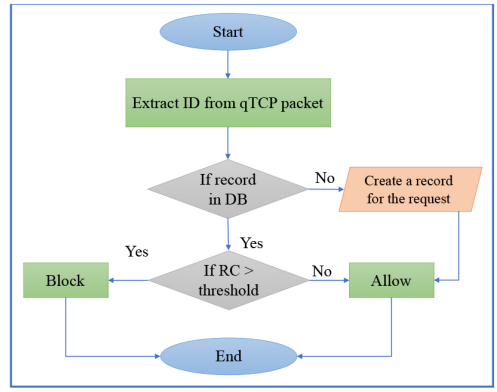

Fig. 8. The Quantum-Firewall Flowchart

IV. Result and Discussion

A. The First Case: All Nodes are Normal

In this case, all quantum nodes are functioning normally and in accordance with the settings prepared for the quantum devices. Every two neighboring nodes can perform quantum entanglement between their respective quantum memories, forming a quantum link between them based on the probability of generating quantum bits in each node as shown in Fig. 9. The entanglement process is completed through a quantum three-way handshake among the generated qubits with the highest probability.

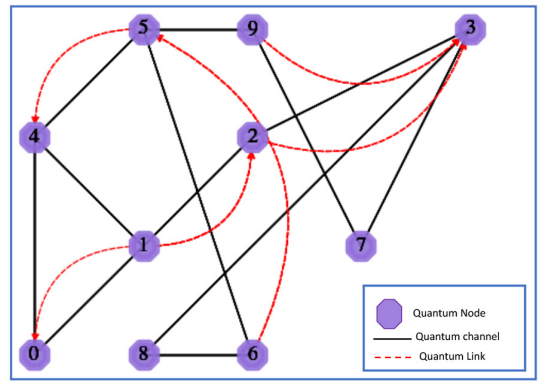

Fig. 9. Establishing Quantum Links Between the Quantum Nodes

B. The Second Case: There is an Attack on the Network in The Absence of a Firewall

The network in this case comprises of 10 quantum nodes, out of which three have been designated as deceptive nodes while the others are normal nodes. These three nodes are identified as 1, 5, and 7, and each node is connected to its neighboring nodes. Table 1 presents the results of the attack on the network, including the number of connections of each node and the number of pairs of entangled quantum bits (EPR) that are prepared at each attacking node. It has been observed that the number of these pairs is equal to or greater than the normal limit for each normal node.

TABLE I
THE COUNT OF CONNECTIONS AND EPRS GENERATED BY DECEITFUL NODES

Deceptive Nodes	Connections	EPRs
1	3	9
5	3	9
7	2	6

Additionally, Table 2 illustrates the encoding of the pairs of quantum bits (Entangled bits) that are prepared at each attacking node with the intention of sending one individual from each pair to the neighboring nodes to which it is connected.

For ease of work, the entanglement pair between two nodes was encoded with a symbol containing the node number and the qubit number. For example, there are 3 qubits generated between node 7 and node 3, and therefore the encoding of these qubits was as follows: |7030>, |7131>, |7232>. Where 7, and 3 represent the number of the two nodes, while 0, 1, 2 represent three different qubits, and so on for the rest of the symbols.

TABLE II
THE ENCODING OF THE PREPARED ENTANGLED BITS PAIRS

Deceptive Nodes	Neighboring Nodes	EPRs Encoding
1	0	|1000>, |1101>, |1202>
	2	|1320>, |1421>, |1522>
	4	|1640>, |1741>, |1842>
5	4	|5040>, |5141>, |5242>
	6	|5360>, |5461>, |5562>
	9	|5690>, |5791>, |5892>
7	3	|7030>, |7131>, |7232>
	9	|7390>, |7491>, |7592>

Moreover, Table 3 reflects the behavior of the quantum attack, listing the details of the connection establishment request packets when the scenario is run for five minutes. This table shows the stability of the packet type, represented by "q-SYN". Additionally, during each second, each deceptive node sends packets containing its identifier and one member of the pairs of the prepared entangled bits for all connected nodes simultaneously.

TABLE III
THE QUANTUM ATTACK BEHAVIOR

First coherent time			
Deceptive Nodes	1	5	7
Request Packets	(q-SYN,|00>,1) (q-SYN,|01>,1) (q-SYN,|02>,1) (q-SYN,|20>,1) (q-SYN,|21>,1) (q-SYN,|22>,1) (q-SYN,|40>,1) (q-SYN,|41>,1) (q-SYN,|42>,1)	(q-SYN,|40>,5) (q-SYN,|41>,5) (q-SYN,|42>,5) (q-SYN,|60>,5) (q-SYN,|61>,5) (q-SYN,|62>,5) (q-SYN,|90>,5) (q-SYN,|91>,5) (q-SYN,|92>,5)	(q-SYN,|30>,7) (q-SYN,|31>,7) (q-SYN,|32>,7) (q-SYN,|90>,7) (q-SYN,|91>,7) (q-SYN,|92>,7)
Second coherent time			
Deceptive Nodes	1	5	7
Request Packets	(q-SYN,|00>,1) (q-SYN,|01>,1) (q-SYN,|02>,1) (q-SYN,|20>,1) (q-SYN,|21>,1) (q-SYN,|22>,1) (q-SYN,|40>,1) (q-SYN,|41>,1) (q-SYN,|42>,1)	(q-SYN,|40>,5) (q-SYN,|41>,5) (q-SYN,|42>,5) (q-SYN,|60>,5) (q-SYN,|61>,5) (q-SYN,|62>,5) (q-SYN,|90>,5) (q-SYN,|91>,5) (q-SYN,|92>,5)	(q-SYN,|30>,7) (q-SYN,|31>,7) (q-SYN,|32>,7) (q-SYN,|90>,7) (q-SYN,|91>,7) (q-SYN,|92>,7)
Last coherent time			
Deceptive Nodes	1	5	7
Request Packets	(q-SYN,|00>,1) (q-SYN,|01>,1) (q-SYN,|02>,1) (q-SYN,|20>,1) (q-SYN,|21>,1) (q-SYN,|22>,1) (q-SYN,|40>,1) (q-SYN,|41>,1) (q-SYN,|42>,1)	(q-SYN,|40>,5) (q-SYN,|41>,5) (q-SYN,|42>,5) (q-SYN,|60>,5) (q-SYN,|61>,5) (q-SYN,|62>,5) (q-SYN,|90>,5) (q-SYN,|91>,5) (q-SYN,|92>,5)	(q-SYN,|30>,7) (q-SYN,|31>,7) (q-SYN,|32>,7) (q-SYN,|90>,7) (q-SYN,|91>,7) (q-SYN,|92>,7)

However, when the coherence time ends, the deceptive nodes continue to resend packets in the same way. This action occupies the communication channels of all connected nodes and consumes quantum memories by keeping the entanglement process incomplete. This incomplete half-quantum communication disrupts the measurement process and prevents then normal nodes from using quantum channels or memories for other quantum communications, ultimately causing network disruption.

Furthermore, Fig. 10 provides a clearer explanation of the requests that are transmitted from every malicious node to the nodes that are adjacent to it.

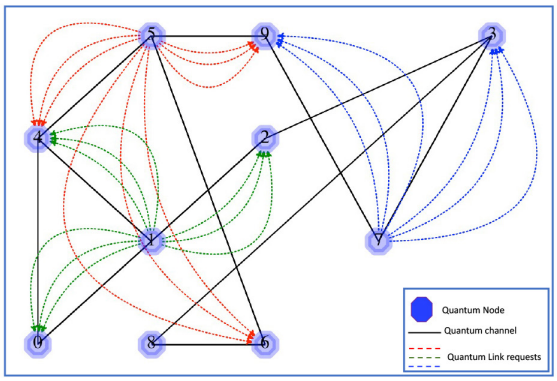

Fig. 10. q-SYN Requests Sent from Malicious Node to Its Neighboring Nodes

C. Third case: There is an attack on the network and the firewall has been activated.

The presence of the firewall in this case mitigates the impact of the DDoS attack, as it examines the received quantum packets (qTCP) and takes countermeasures against the attack. The results of activating the quantum firewall on quantum devices are shown in Table 4. It is clear from this table that the rules applied to the packets allow the quantum packets to be received and passed to the node to conduct quantum communication between the nodes only twice (as a threshold). Accordingly, the quantum firewall prevents nodes from receiving any packets belonging to a specific node when these

requests are repeated twice or more than that immediately after the coherence time expires. That is, when the coherence time ends and deceptive nodes re-send the same packets every time, the firewall in this case will prevent receiving any packets coming from these deceptive nodes.

TABLE IV
THE QUANTUM FIREWALL BEHAVIOR

Deceptive Nodes	1	5	7
Adjacent Nodes	0	4	3
Request Packets	(q-SYN,|00>,1) (q-SYN,|01>,1) (q-SYN,|02>,1)	(q-SYN,|40>,5) (q-SYN,|41>,5) (q-SYN,|42>,5)	(q-SYN,|30>,7) (q-SYN,|31>,7) (q-SYN,|32>,7)
Coherent Time	1	2	More than 2
Count Action	Allow	Allow	Deny

Finally, the firewall effectively decreased the number of requests being sent to the quantum nodes, resulting in maintain the availability of the quantum network.

V . CONCLUSION

This work has clarified two aspects of the quantum network. Firstly, it showed a method of attacking the network by employing the quantum TCP-three-way handshake connections. The other aspect was to defend against this attack or mitigate it by proposing and implementing a quantum firewall. From this work, we can conclude that according to quantum laws, the attack cannot be from outside the network due to the agreements prepared in advance in order to create quantum entanglement between quantum devices. Additionally, we can say that the quantum attack has an impact on the availability of the network, as each node performs an attack, it affects the quantum channels and memories in every node connected to it. This consumption of quantum bits prepared to create quantum links with other nodes causes the network to stop working as this action continues on all devices in the network.

Finally, when implementing a security method, it can be concluded that it can mitigate the impact of the attack and maintain availability. The firewall mainly depends on the ID of each quantum node as well as the coherence time of the quantum memories.

REFERENCES

[1] S. A. Hussein and A. A. Abdullah, "A comprehensive study of the basics of quantum networks," *2022 5th International Conference on Engineering Technology and Its Applications (IICETA)*, May 2022, DOI: 10.1109/IICETA54559.2022.9888324.

[2] L. Zhonghui, X. Kaiping, L. Jian, C. Lutong, L. Ruidong, W. Zhaoying, Y. Nenghai, W. David, S. Qibin, and L. Jun, "Entanglement-Assisted Quantum Networks: Mechanics, Enabling Technologies, Challenges, and Research Directions," in *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2133–2189, 2023, DOI: 10.1109/COMST.2023.3294240.

[3] K. Adarsh, B. Surbhi, K. Keshav, G. S. Manjula, D. S. Gayathri, D. J. Pacheco, A. Diego and M. Arwa, "Survey of Promising Technologies for Quantum Drones and Networks," in *IEEE Access*, vol. 9, pp. 125 868–125 911, 2021, DOI: 10.1109/ACCESS.2021.3109816

[4] P. Bhattacharyya, H. Sastry, V. Marriboyina and R. Sharma, *Smart and Innovative Trends in Next Generation Computing Technologies*. India: Springer, 2017, DOI: 10.1007/978-981-10-8657-1

[5] B. A. Huberman and B. Lund, "A quantum router for the entangled web," *Information Systems Frontiers*, vol. 22, no. 1, pp. 37–43, Dec. 2019, DOI: 10.1007/s10796-019-09955-5

[6] S. A. Hussein and A. A. Abdullah, "Hybrid routing protocol for quantum network based on classical and quantum routing metrics," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 1, p. 197, Jul. 2023, DOI: 10.11591/ijeecs.v31.i1.

[7] T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdušek, and R. Van Meter, "Attacking the quantum internet," *IEEE Transactions on Quantum Engineering*, vol. 2, pp. 1–17, Jan. 2021, DOI: 10.1109/TQE.2021.3094983

[8] H. Zhou, K. Lv, L. Huang, and X. Ma, "Quantum Network: security assessment and key management," *IEEE ACM Transactions on Networking*, vol. 30, no. 3, pp. 1328–1339, Jun. 2022, DOI: 10.1109/TNET.2021.3136943

[9] P. Burdiak *et al*., "Use-Case Denial of Service Attack on Actual Quantum Key Distribution Nodes," *In Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023)*, Jan. 2023, DOI: 10.5220/0011672000003405

[10] F.-H. Hsu, Y. L. Hwang, C. Tsai, W. T. Cai, C.-H. Lee, and K. W. Chang, "TRAP: a Three-Way handshake server for TCP connection establishment," *Applied Sciences,* vol. 6, no. 11, p. 358, Nov. 2016, DOI: 10.3390/app6110358

[11] Q.-M. Ma, S. Liu, and X. Wen, "TCP Three-Way Handshake Protocol based on Quantum Entanglement," *Journal of Computers,* pp. 033–040, Oct. 2016, DOI: 10.3966/199115592016102703004

[12] N. Yu, C.-Y. Lai, and L. Zhou, "Protocols for packet Quantum network intercommunication," *IEEE Transactions on Quantum Engineering,* vol. 2, pp. 1–9, Jan. 2021, DOI: 10.1109/TQE.2021.3112594

[13] R. Ursin *et al*., "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, no. 7, pp. 481–486, Jun. 2007, DOI: 10.1038/nphys629.

[14] Z. Li et al., "Entanglement-Assisted Quantum Networks: mechanics, enabling technologies, challenges, and research directions," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 4, pp. 2133–2189, Jan. 2023, DOI: 10.1109/comst.2023.3294240.

[15] J. Clarke and F. K. Wilhelm, "Superconducting quantum bits," *Nature,* vol. 453, no. 7198, pp. 1031–1042, Jun. 2008, DOI: 10.1038/nature07128.

[16] B. Nordén, "Quantum entanglement: facts and fiction – how wrong was Einstein after all?," *Quarterly Reviews of Biophysics*, vol. 49, Jan. 2016, DOI: 10.1017/s0033583516000111.

[17] R. Demkowicz-Dobrzański, A. Sen, U. Sen, and M. Lewenstein, "Entanglement enhances security in quantum communication," *Physical Review A*, vol. 80, no. 1, Jul. 2009, DOI: 10.1103/physreva.80.012311.

[18] A. Wallucks, I. Marinković, B. J. Hensen, R. Stockill, and S. Gröblacher, "A quantum memory at telecom wavelengths," *Nature Physics*, vol. 16, no. 7, pp. 772–777, May 2020, DOI: 10.1038/s41567-020-0891-z.

[19] H. M. Mohammad and A. A. Abdullah, "DDoS attack mitigation using entropy in SDN-IoT environment," *AIP Conference Proceedings*, Jan. 2023, DOI: 10.1063/5.0123465.

[20] Y. Jassem, and A. Abdulkareem. "Enhancement of quantum key distribution protocol for data security in cloud environment."*Icic International*, vol. 11, no. 3, pp. 279–288, 2020, DOI: 10.24507/icicelb.11.03.279

[21] S. S. Mahdi and A. A. Abdullah, "Enhanced Security of Software-defined Network and Network Slice Through Hybrid Quantum Key Distribution Protocol" *Infocommunications Journal*, vol. 14, no. 3, pp. 9–15, 2022, https://doi.org/10.36244/ICJ.2022.3.2

[22] A. Furusawa and P. Van Loock, *Quantum Teleportation and Entanglement: A hybrid approach to optical quantum information processing*. New York: John Wiley & Sons, 2011. DOI: 10.1002/9783527635283.ch8

[23] A. Singh, K. Dev, H. Šiljak, H. D. Joshi, and M. Magarini, "Quantum Internet—Applications, functionalities, enabling technologies, challenges, and research directions," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, pp. 2218–2247, Jan. 2021, DOI: 10.1109/comst.2021.3109944.

[24] J. M. Kizza, *Guide to computernetwork Security*, 6th ed. Berlin: Springer, 2024. DOI: 10.1007/978-3-031-47549-8.

Shahad A. Hussein is currently serving as an Assistant Lecturer at the University of Babylon in the College of Information Technology, located in Babylon, Iraq. She graduated with a Bachelor's degree in Information Technology with excellent grades, ranking first in her class from Babylon University in 2016. In 2017, she was awarded the first place at the national level for the Iraqi Science Day Award for her exceptional graduation research in her field of study. In 2022, she completed her M.Sc. degree from the College of Information Technology at Babylon University. Her current research field focuses on Quantum networks, Network Security, and various aspects related to the future internet.

Suadad S. Mahdi presently serves as a Lecturer at the University of Babylon, specifically within the College of Information Technology in Babylon, Iraq. Her academic journey includes earning a Bachelor's degree in Information Technology from Babylon University in 2016, followed by a Master's degree in Information Networks from the College of Information Technology (IT) in 2020. In 2024, she successfully completed her PhD in Information Networks from the same college. Currently, Suadad's research focuses on a wide range of topics, encompassing future internet, NFV, SDN, network security, cryptography, and quantum cryptography.

Alharith A. Abdullah received his B.S. degree in Electrical Engineering from Military Engineering College, Iraq, in 2000. MSc. degree in Computer Engineering from University of Technology, Iraq, in 2005, and his PhD. in Computer Engineering from Eastern Mediterranean University, Turkey, in 2015. His research interests include Security, Network Security, Cryptography, Quantum Computation and Quantum Cryptography.