Virtual Private Network—Firewall Integration for Wireless Local Area Network Improvement against Jammers

Shayma W. Nourildean
Communication Engineering Department, University of Technology, Baghdad, Iraq
Email: Shayma.w.nourildean@uotechnology.edu.iq (S.W.N.)

Abstract*—Wireless networks are susceptible to many security problems since the wireless medium is open. Jammer (jamming attack) is the most important problems in wireless networks. It is denial-of-service attack in which attackers send malicious signals or messages on a channel that is intended for normal traffic by intentionally interfering with the network. One of the solutions is the development of tunneling technology as an attempt to secure communication networks. Virtual Private Network (VPN) tunneling technology when integrated with firewall would provide a suitable security. In this study, number of Jammers would interfere with the normal operation of the network resulting in performance degradation of network. These Jammers decrease throughput and increase delay and data dropped. The aim of this study is to improve the performance of Wireless Local Area Network (WLAN) by integrating Firewall with VPN in number of different Riverbed Modeler simulation scenarios which it is utilized in this study for video and data applications. Firewall is a technology employed to regulate the level of network connectivity. It can block unauthorized access from an external network to an internal network's resources. In this study, the tunneling technology of VPN was integrated with firewall to improve the performance by increasing the throughput and decreasing delay and data dropped. The firewall would block any access to the server from the workstations and the VPN would filter the packets to allow a specific access to the specific server. The results showed that VPN when integrated with firewall increased the throughput from 1,350,000 to 1,500,000 bits/sec and decreased the delay from 0.0054 sec to 0.0047 sec and data dropped from 7,800 to 5,000 bits/sec so that this study proved that VPN incorporated with firewall provides a good throughput and delay improvement for wireless local area network.

***Index Terms*—Virtual Private Network (VPN), firewall, Wireless Local Area Network (WLAN), Jammers, riverbed**

I. Introduction

Wireless networks enable communication between one or more devices without the requirement for network or peripheral cables or physical connections. They transmit data through radio frequency transmissions, as opposed to wired systems, which do it using cables [1]. Wireless Local Area Network (WLAN) has geographical coverage restrictions but offers a higher bandwidth for data communication. IEEE 802.11(a, b, c), also known as WiFi, (Wi-Fi Alliance) is currently a viable technology for wireless LANs and has been widely used for resource sharing and data exchange [2, 3]. Wireless communications and equipment are practical, adaptable, and simple to use, according to several organizations and users [4]. Wireless networks are susceptible to many security problems since a wireless medium is open. Jammer (jamming attack) is the most important problems in wireless networks. It is denial-of-service attack in which attackers send malicious signals or messages on a channel that is intended for normal traffic by intentionally interfering with the network [5]. VPN (Virtual Private Network) technology is utilized for encrypted communications between organizations based at various locations across the world [6]. In this study,

- the Jammers interfere with the normal operation of network and degrade the network's performance by decreasing the throughput and increasing delay and data dropped.
- the WLAN performance had been improved in this study using the tunneling technology of VPN and firewall.
- In different Riverbed Modeler scenarios, the firewall would block any video and data access to the server from the workstations and the VPN would filter the packets to allow a specific video and data access to the specific server which resulted in increasing throughput and decreasing delay and data dropped.
- The performance had been investigated in terms of delay, throughput and data dropped parameters.
- This network platform is simulated using (Riverbed academic edition 17.5).

The structure of the paper is: Section II presented literature review about the previous studies, Section III described some definitions of the theoretical basis for this study, Section IV described the research methodology used to collect the results which it is presented in Section V as well as the discussion and Section VI described the conclusions.

Manuscript received June 14, 2023; revised September 21, 2023; accepted October 14, 2023; published February 2, 2024.

doi: 10.18178/ijeetc.13.1.58-66

II. Literature Review

A review of jamming assaults was presented by Jasim *et al.* [7], focusing on several strategies to identify and thwart these attacks. Additionally, a number of defenses have been put out to counteract jamming attempts, including the use of jamming-resistant protocols and the incorporation of anti-jamming algorithms into wireless devices. A jammer attack module is suggested by Bout *et al.* [8] utilizing Network Simulator-3 (NS-3). This platform create an intelligent channel hopping mechanism and a jamming attack based on prior efforts to show its scalability. Obaid *et al.* [9] performed jamming assaults using OPNET Modeler in order to study the behavior of wireless networks. The findings demonstrated that the researched jamming attacks may seriously impair the operation of wireless networks, and that channel switching technique could effectively prevent jamming attackers. He [10] improved our understanding of firewall technologies for computer networks. Manikanthan *et al.* [11] examined the effectiveness of numerous deep learning models in identifying interference and jamming signals in order to study the different signal features that could be utilized to detect jamming and interference signals. Maghsoudlou *et al.* [12] identified and classified VPN servers in the wild, which makes it easier to identify VPN traffic and examine their cryptographic certifications, vulnerabilities, physical locations, and fingerprints. Pirayesh *et al.* [13] provides a comprehensive overview of interference attacks and countermeasures for Wi-Fi, cellular, Bluetooth and GPS wireless networks and an analysis of extant jamming strategies and defense mechanisms. Xu *et al.* [14] aimed to look into how movable Jammers effect WSNs. The reliability and performance of WSN are significantly impacted by the jammer's movement, according to simulation studies. To keep WSN functioning normally, local and global maintenance procedures for sensor nodes must be designed. Yao and Zhu [15] examined endogenous anti-jamming (EAJ), a powerful defense against unidentified electromagnetic attacks, as one of the core challenges of endogenous security in the electromagnetic domain, the fundamental idea, important strategies, and development recommendations of wireless communication endogenous anti-jamming are put out. In a variety of distinct Riverbed Modeler Simulation situations for various audio and video applications, Nourildean *et al.* [16] decreased the performance degradation brought on by Jammers by using three ad hoc routing protocols (AODV, GRP, and OLSR). The outcomes demonstrated that these routing algorithms significantly impacted network performance. A machine-learning method to defend against jamming assaults in underwater networks was presented by Mertens *et al.* [17] This applies to security applications where sensor devices are placed in high-risk areas. The proposed approach is efficient in reducing unnecessary energy use, according to extensive simulation and performance research.

These works in the recent years presented review of jamming attacks and detection of jamming to find anti-jamming strategy for wireless network. Some of these works examined the utilization. Some of these works examined the impact of Jammers on other networks like Wireless Sensor Networks (WSN). In this paper, the integration of VPN and firewall as an anti-jamming strategy was examined to improve the QoS (Quality of Service) parameters (Delay, throughput and packet loss) of the wireless network in different traffic loads like data and video applications.

III. Theoretical Basis

A. Wireless Local Area Networks (WLAN)

Since the development of affordable, high-performance Wireless Local Area Network (WLAN) technology, many real-world applications use wireless control. From a systems design standpoint, the prospect that each mobile node might be viewed as a node on a LAN is particularly desirable when a lot of mobile nodes must cooperate [18]. WLANs are collections of radio-capable wireless networking nodes that are located in a specific region, like a campus or office building. In order to improve user mobility, WLANs are typically installed as extensions to already-existing wired local area networks. 802.11, Hiper LAN (Local Area Network), and a number of additional protocols are examples of WLAN [1]. Wi-Fi technology, also known as wireless fidelity, was created by IEEE 802.11 standards in 1997 and gave consumers the freedom for faster wireless access to Internet applications from any location. For Wi-Fi Technology to function, radio frequencies like 2.4GHz and 5GHz require wireless components like the Ethernet protocol and CSMA (Carrier Sense Multiple Access). This approach uses a wireless router or hotspot as the transmitter and any Wifi-enabled device as the receiver, just like any other communication network. Wireless communications and gadgets are practical, adaptable, and simple to use, according to numerous organizations and users. With the use of WLAN devices, users can move their laptop computers around their offices while still connected to the network [4]. Due to its fast data rates, simple implementation, and low cost, IEEE 802.11 WLAN has become one of the most widely used wireless technologies in indoor settings. However, the 802.11 WLAN system's transmission ranges have been constrained by the high frequency bands, and as a result, the system has received little attention in outdoor settings [19].

B. Wireless Standards

WiFi is the most popular technology for the IEEE 802.11 WLAN standard which has become necessary in modern life. Nearly 100 billion IoT devices, tablets, smart phones, desktops, laptops, video cameras, smart TVs, printers, monitors, and other consumer electronics had been connected by more than a billion access points to the Internet, allowing large applications to be used anywhere, by everyone [20]. There are various Wi-Fi Standards for different data rates [4].

C. Security Vulnerabilities in Wireless Networks

Due to the global deployment of services, the increased need for faster data rates, the need for cutting-edge services like roaming, wireless communications vulnerabilities are growing. As a result, there are now extremely difficult challenges with the security of wireless systems and applications in wireless environments. The security of wireless communications is any procedure to stop unauthorized access to or loss of data transferred via wireless networks, as well as to make sure that the integrity and confidentiality of data are not compromised [21].

D. Jamming Attacks

Jamming is the disruption of ongoing wireless communications at different communication layers in wireless networks. This type of attack often targets the physical layer, and it can be carried out by transmitting high power noise at the appropriate time (time slot), frequency (sub-carriers), and place in order to reduce the Signal-to-Interference-plus-Noise-Ratio (SNR) (close to the receiver or the transmitter). Regular Jammers, which are unable to detect genuine signal power, and smart Jammers, which work by jamming when they detect a transmission on the channel and have the capacity to learn the current signal powers, are the two types of Jammers that are taken into consideration. In the beginning, a smart jammer continuously scans the wireless spectrum to identify the operational frequency range that both parties use for communication. Then, in order to lower the SNR to a predetermined threshold, a signal is sent using that frequency range. Jamming assaults may raise the danger of Denial-of-Service (DoS) attacks, increase communication latency, and decrease energy efficiency DoS [22, 23]. Fig. 1 shows a classification of wireless Jammers.

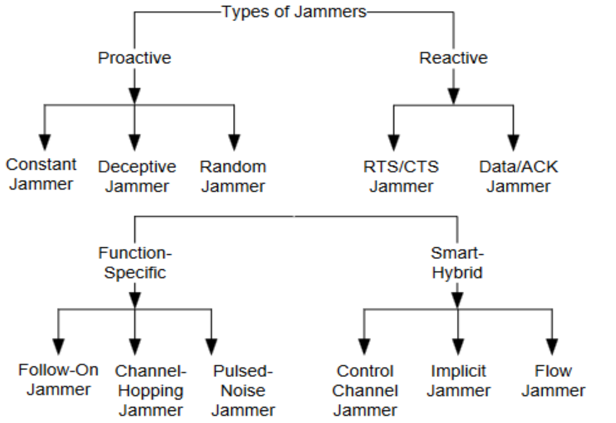

Fig. 1. Jammers types [1].

E. Virtual Private Network (VPN)

VPN is a private point-to-point network that is built over an existing network, such as an Internet Protocol (IP) Network incorporating additional features like encryption, user secrecy, and data protection. By enclosing the communications payload in VPN protocol headers, two peers can create a private point-to-point link. VPN uses cryptographic techniques to encrypt the payload as well. Gateway to gateway and dial-up VPN architectures are two examples of VPN architectures. The following tunneling protocols are used by VPN: Secure Socket, Layer-2 Tunneling Protocol, Point to Point Tunneling Protocols and Internet Protocol security [6]. The essence of VPN is to establish a network tunnel using encryption technology in a public network to safely carry out directional data transmission and prevent others from sniffing [24]. Fig. 2 and Fig. 3 shows how VPN works.

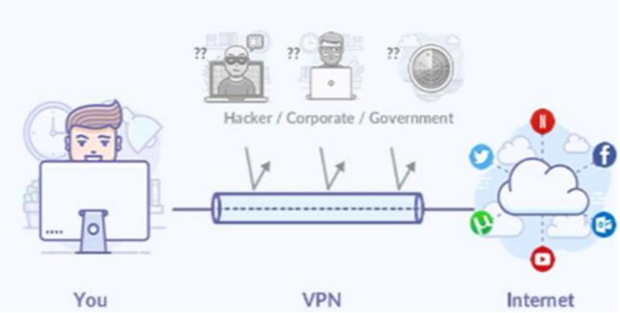

Fig. 2. How does VPN works? [25].

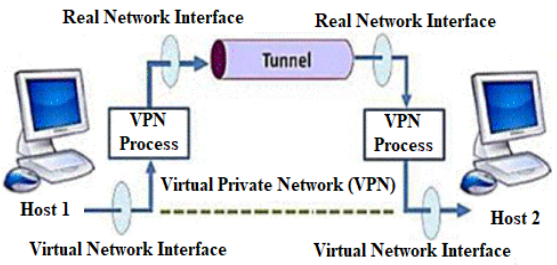

Fig. 3. VPN [26].

- ➢ Types Of VPN [27]:
  - Site to Site VPN (Based on Internet)
  - Site to Site VPN (Based on Extranet)
  - Remote Access VPN.
- ➢ Advantages of VPN [25]
  - VPNs remove geographic limitations.
  - Online privacy is no longer in danger, and it safeguards against thieves.
  - Transfer of data is secured.
  - You can use the public network to tunnel a private connection to the internet using only regional leased lines, cable networks, or both.
  - Saving money.
- ➢ VPN Devices [27]:
  - Hardware

A hardware VPN that is based on a lone, independent device. The device's dedicated processor controls the hardware firewall and other VPN features, including authentication and encryption [27].

- Firewall

A technology called a firewall is employed to regulate the level of network connectivity. It can block unauthorized access from an external network to an internal network's hardware and networks' resources. This indicates that a firewall can defend an internal network from possible network attack risks. Where there are VPNs, there are always firewalls as well. Our data is protected from data hunters due to the fact that all external Internet traffic is routed through this tunnel. VPNs are methods of accessing the internal network, while firewalls serve as the gateway to ensure the security of the internal network. Without a firewall, a VPN loses its ability to encrypt data. The security of the Internet and the network generally is increased by using VPN in conjunction with firewall [28, 29].

- Software:

The user's network does not change, which is the main benefit of the software approach. No additional hardware must be installed, and network administration is unchanged [27].

IV. Research Method

A commercial GUI (Graphical User Interface) simulation application called Riverbed Modeler's Academic Version 17.5 is used to study different networks. It is an OPNET Modeler (14.5) newer academic edition that enables users to graphically design the topology of networks. to determine the performance of the network in different scenarios [30, 31].

In this paper, a number of jamming attacks interfere with the network's normal operation so that they increased packet loss and delay and decreased the throughput. The aim of this study is to improve the performance of the WLAN using the virtual private network with firewall. Delay, Packet loss (data dropped) parameters were measured for video and data access parameters. The simulation setup consists of four scenarios to represent each case of the network. The research simulation steps are as follows:

- Each scenario had 36 wireless workstations connected to three access points (AP1, AP2 and AP3).
- The three access points specified by wireless ethernet IP router is connected to the IP cloud to access the servers (Server 1, Server 2)
- Point to point links and 100 Mbps (Mega bits per second) duplex links connect the objects in each scenario.
- Application definition is specified for all applications.
- Profile configuration is defined for video and data access applications
- Assign each workstation and server to the application and profile configuration.
- Five Jammers interfered with the normal operation of the network.
- Firewall is applied to block any access to the server.
- VPN is configured to allow specific access from the specific workstation to specific server.
- Discrete Event Statistics (DES) had been chosen for WLAN statistics.
- Run the simulation for 1,200 s.

The scenarios are as follows:

- Scenario 1 (WLAN): in this scenario, the workstations are connected to three access points which are connected to the IP cloud to access the servers (1 and 2). This case is shown in Fig. 4.
- Scenario 2 (WLAN): in this scenario, five Jammers interfere with the network and cause the network degradation in performance. This case is shown in Fig. 5.
- Scenario 3 (WLAN_Firewall_Jammers): in this scenario, Firewall is applied to block any access to the Sever as a try to protect the servers from an authorized access. This case is shown in Fig. 6.
- Scenario 4 (WLAN_Frewalls_VPN_Jammers): in this scenario, the VPN is configured to allow specific video or data access from specific Access Point (AP2) to a specific destination (Server 1). This case is shown in Fig. 7.

After choosing the required parameters and running the simulation, the results had been collected in next section.

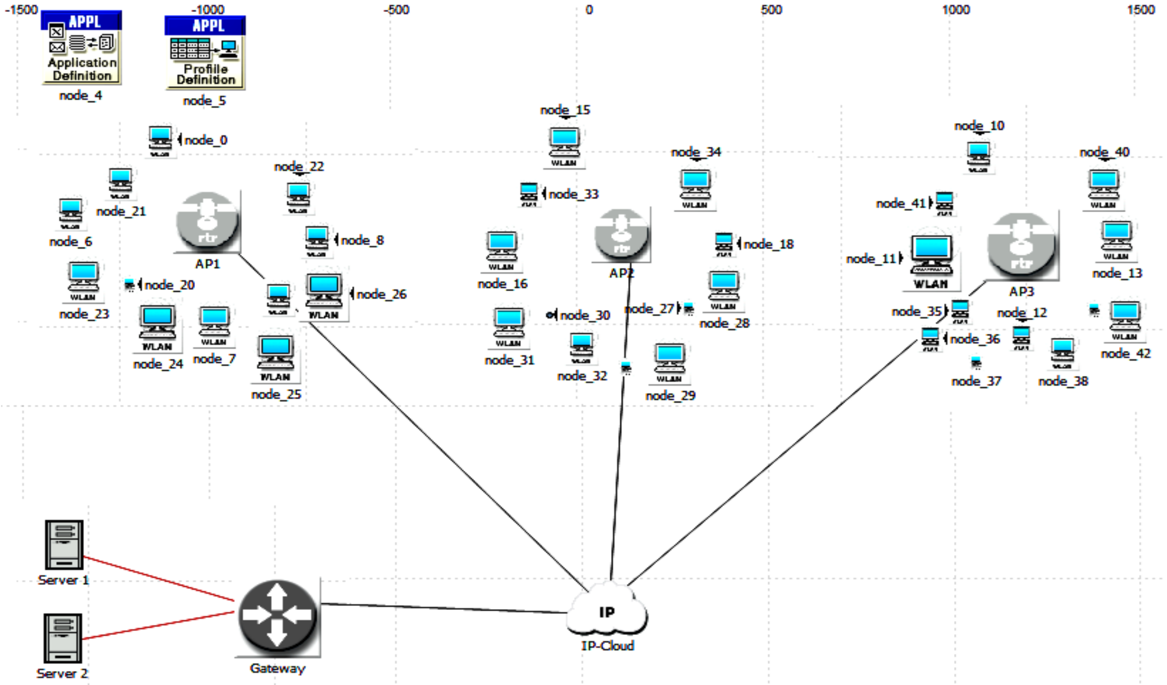

Fig. 4. WLAN without Jammers.

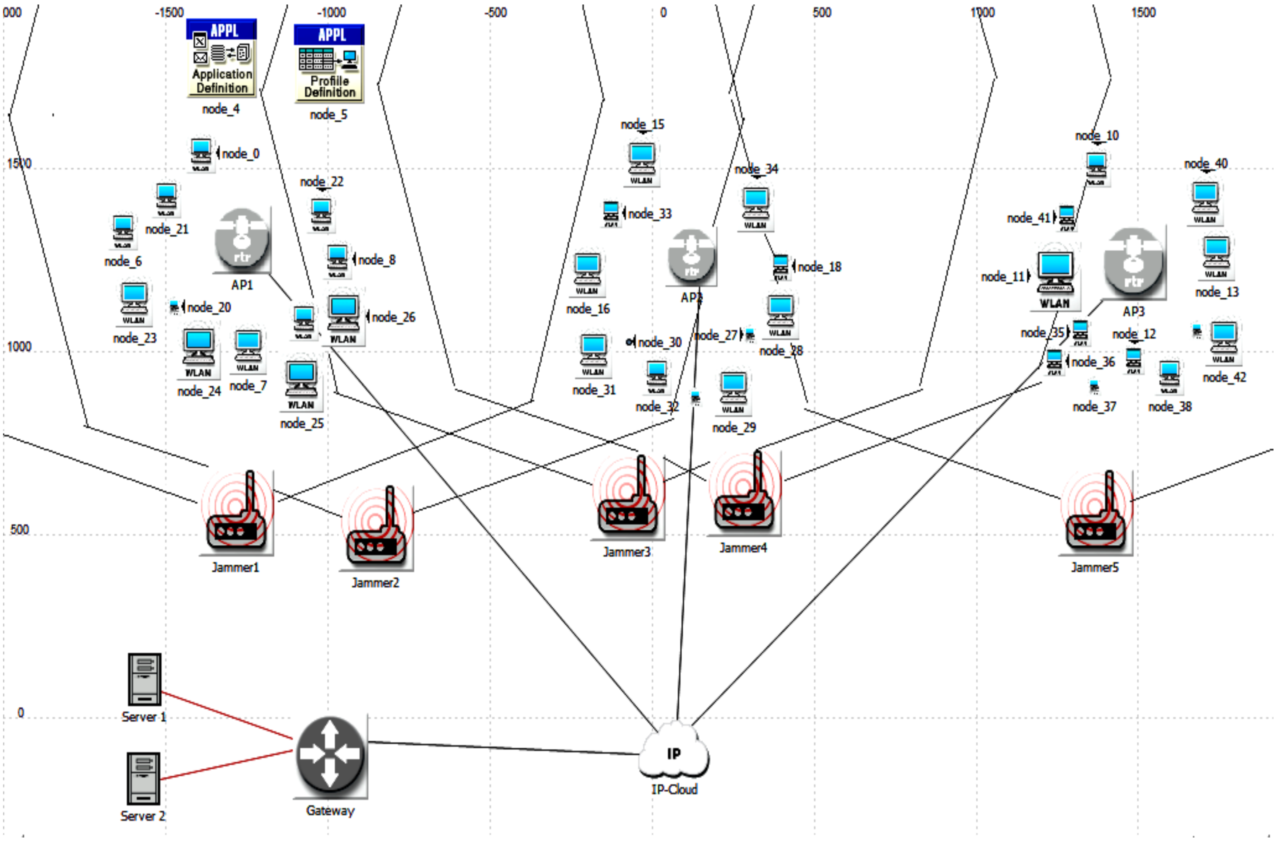

Fig. 5. WLAN_Jammers.

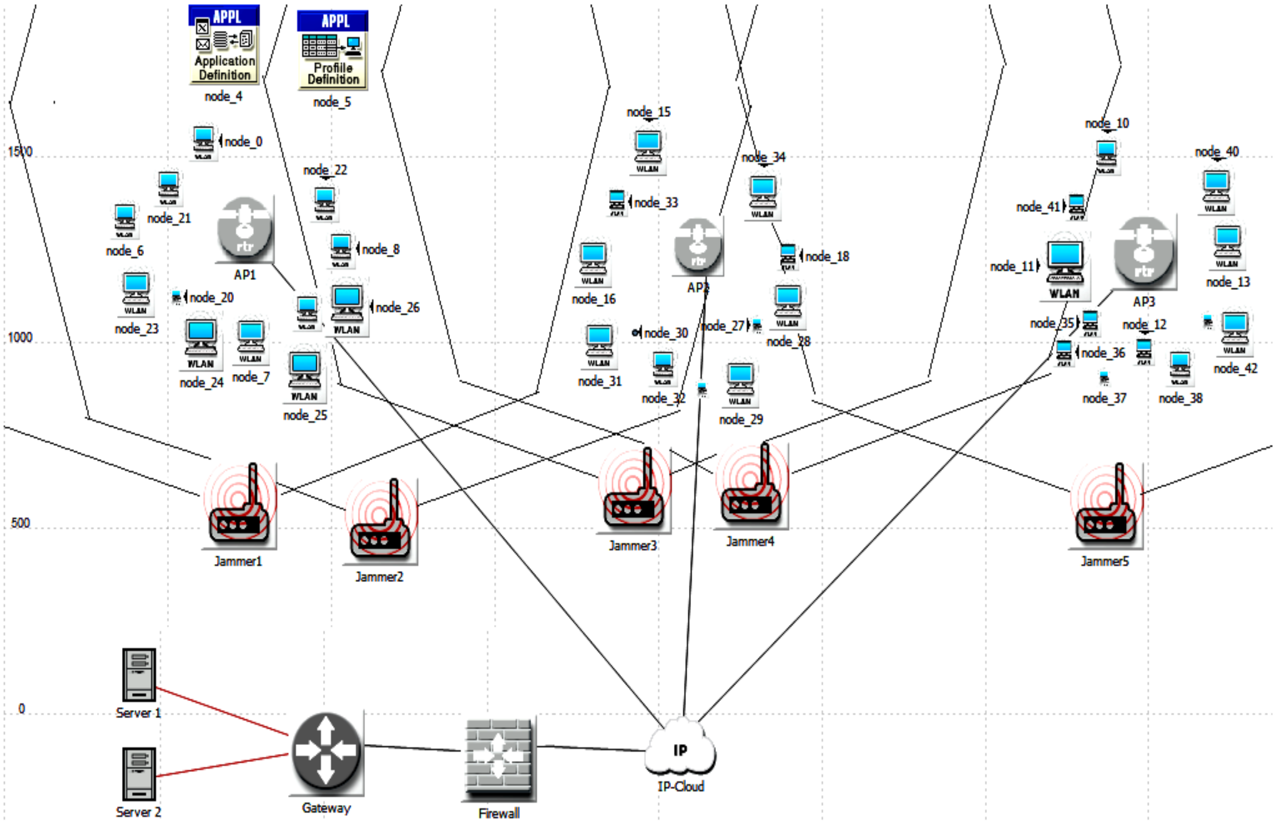

Fig. 6. WLAN_Firewall_Jammers.

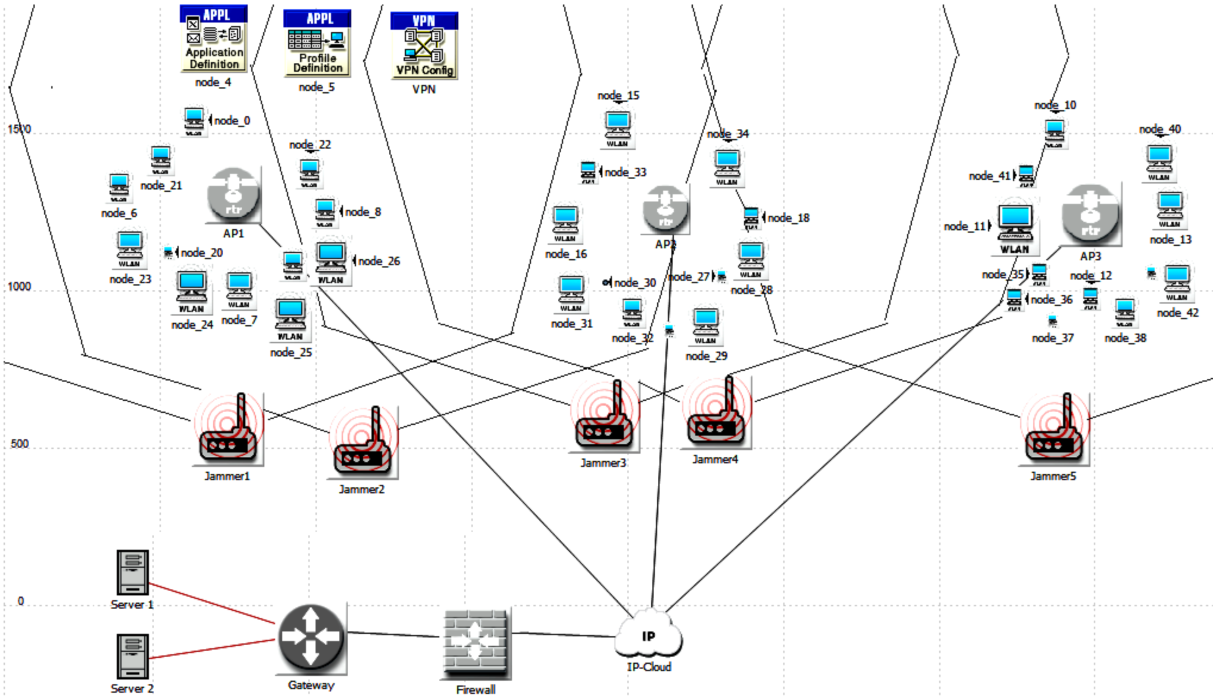

Fig. 7. WLAN_Frewalls_VPN_Jammers.

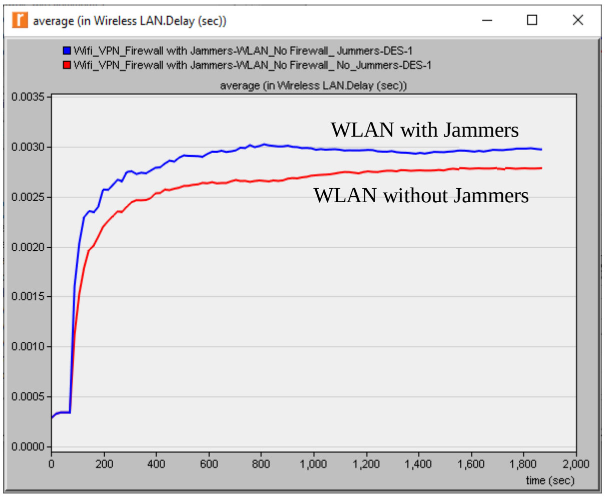

Fig. 8. Delay of the network with and without Jammers.

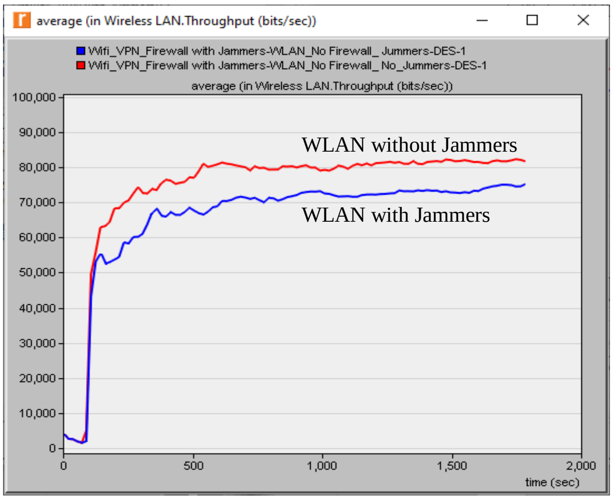

Fig. 9. Throughput of the network with and without Jammers.

V. Results and Discussion

The simulation is run for 1,800 s to collect the results as follows:

- Delay: It specifies the time it takes for a packet of data to travel from one communication endpoint to another across the network. The delay is measured for two cases with Jammers and without Jammers to examine how the performance of network would degrade in the existence of Jammers as shown in Fig. 8. Typically, it is measured in fractions or multiples of a second.
- Throughput: is the number of information units that a system is able to process in a specified period of time. The throughput is measured for two cases with Jammers and without Jammers to examine how the performance of network would degrade in the existence of Jammers as shown in Fig. 9. Typically, it is measured in bits per second.

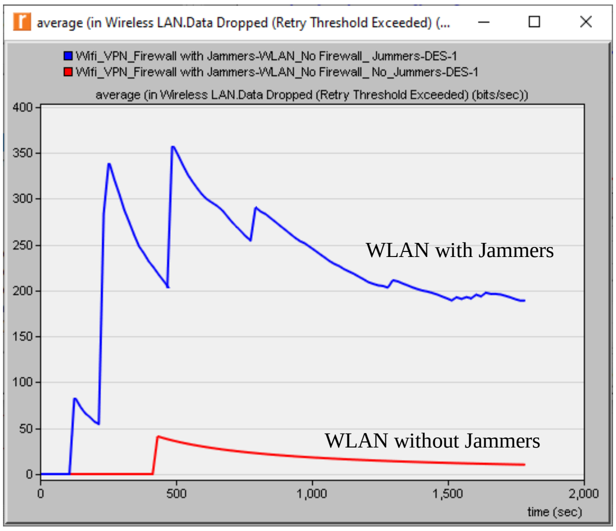

Fig. 10. Data dropped of the network with and without Jammers.

- Data Dropped (Packet Loss): identifies data packets that were transmitted throughout a network but failed to reach their destination. Data dropped is measured for two cases with Jammers and without Jammers to examine how the performance of network would degrade in the existence of Jammers as shown in Fig. 10. Typically, it is measured in bits per second.

The jammers interfere with the normal operation of the network so that the existence of five Jammers increased the dropping of data and the delay and decreased the throughput leading to the result that the Jammers degrade the performance of the network.

The impact of Firewall and VPN was examined to improve the performance deficiency caused by the Jammers.

- Delay was measured for the three cases to examine the performance of the network with Jammers, with firewall only and firewall integrated with VPN as shown in Fig. 11.

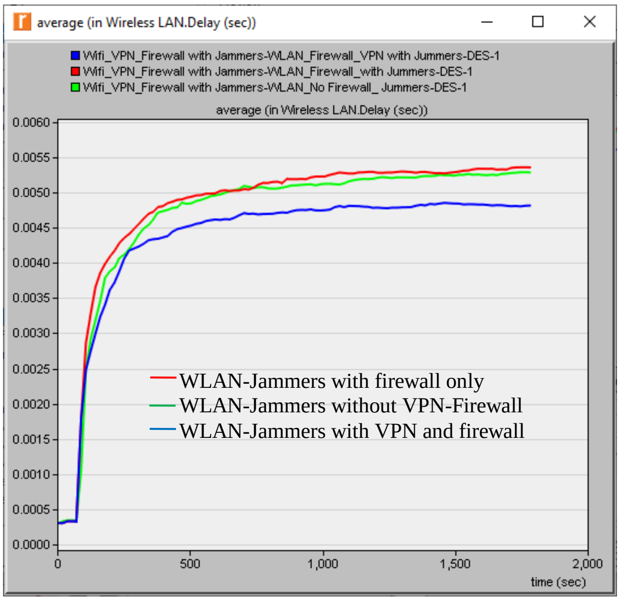

Fig. 11. Delay of network with the tunneling technology of VPN with firewall.

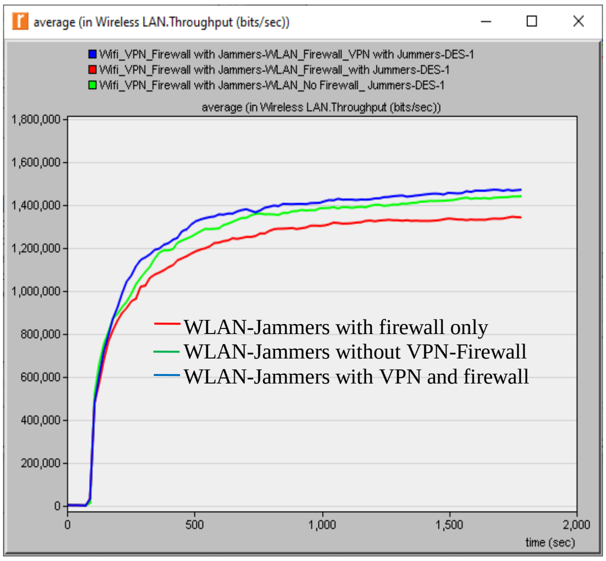

Fig. 12. Throughput of network with the tunneling technology of VPN with firewall.

VPN reduced the delay caused by the Jammers when it is integrated with firewall and this integration resulted in a delay improvement from 0.0054 s to 0.0047 s approximately.

- Throughput was measured for the three cases to examine the performance of the network with Jammers, with firewall only and firewall integrated with VPN as shown in Fig. 12.

VPN increased the throughput which decreased by the Jammers when integrated with firewall from 1,350,000 to 1,500,000 bits/sec, therefore the integration of VPN with Firewall investigated a throughput improvement.

- Data Dropped (Packet Loss) was measured for the three cases to examine the performance of the network with Jammers, with firewall only and firewall integrated with VPN as shown in Fig. 13.

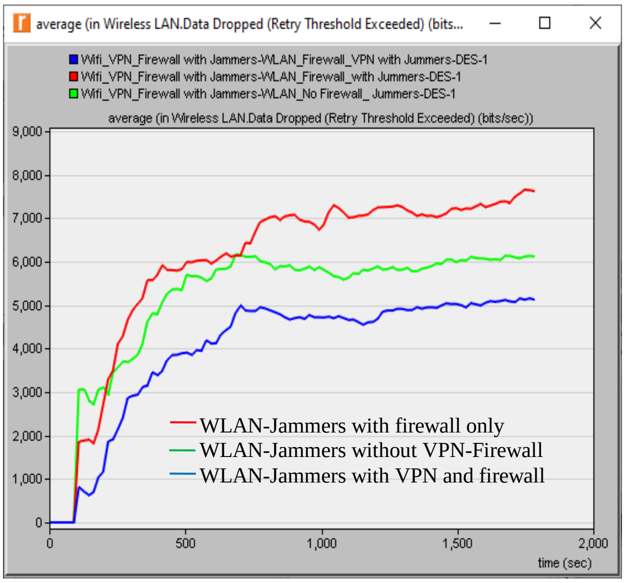

Fig. 13. Data dropped of network with the tunneling technology of VPN with firewall.

VPN reduced the dropping of data caused by the Jammers when it is integrated with and this integration resulted in a packet loss improvement from 7,800 to 5,000 bits/s approximately.

As shown in these figures, firewall with VPN integration would increase the throughput and decrease dropping of data and the delay so that delay, packet loss and throughput improvement would improve the efficiency and the speed of the network.

VI. Conclusion

Wireless networks are vulnerable to many different attacks due to the wireless networks' open nature. Jamming attacks (Jammers) are kinds of Denial-of-Service attack (DoS) which interfere with the normal operation of network which degrade the performance of network. Firewall is one of the related technologies of VPN. It can block unauthorized access to the internal network's hardware and network resources. This indicates that a firewall can defend an internal network from possible network attack risks. VPN technology is utilized for encrypted communications between organizations based at various locations across the world. Without a firewall, a VPN loses its ability to encrypt data. In this paper, a number of Jammers would interfere with the normal operation of the network resulting in decreasing throughput and increasing delay and data dropped (packet loss) so the the aim of this study is to improve the performance of the WLAN by integration VPN with the firewall in number of different scenarios utilizing Riverbed Modeler v17.5 for different video, voice and data access applications. The results showed that the VPN with firewall incorporation would not enable full access to the server because VPN would allow authorized access from specified sender to specified receiver because VPN tunnel would allow the workstations of Access Point 2 (AP2) to access Server 1 for specific applications so that the throughput was increased 1,350,000 to 1,500,000 bits/sec and decreased the delay from 0.0054 s to 0.0047 s and data dropped from 7,800 to 5,000 bits/s. Throughput, delay and data dropped are the major QoS parameters of any network so that VPN when integrated with firewall investigated a good throughput and delay improvement. Future works includes study this integration of VPN-Firewall on other networks like (WSN) for different traffic load in different applications.

Conflict of Interest

The author declares no conflict of interest.

References

[1] M. Dahiya, "Evolution of wireless lan in wireless networks," *Int. J. Comput. Sci. Eng. Evol.*, vol. 9, no. 3, pp. 109–113, 2017.

[2] I. Khan, H. Nawaz, M. M. Rind, K. Kumar, M. A. Chahajro, and A. Mailto, "Comparative study of existing and forthcoming WLAN technologies," *Int. J. Comput. Sci. Netw. Secur.*, vol. 18, no. 4, pp. 101–108, 2018.

[3] E. Lopez-Aguilera, E. Garcia-Villegas, and J. Casademont, "Evaluation of IEEE 802.11 coexistence in WLAN deployments," *Wirel. Networks*, vol. 25, no. 1, pp. 87–104, 2019.

[4] S. Surendra Tambe, "Wireless technology in networks," *Int. J. Sci. Res. Publ.*, vol. 5, no. 7, pp. 1–3, 2015.

[5] S. Djuraev and S. Y. Nam, "Channel-hopping-based jamming mitigation in wireless lan considering throughput and fairness," *Electron.*, vol. 9, no. 11, pp. 1–20, 2020.

[6] A. Jagtap, "Firewall and VPN Technology," *Int. J. Sci. Res.*, vol. 6, no. 12, pp. 1762–1765, 2017.

[7] S. I. Jasim, O. K. Hamid, and N. J. Alhyani, "A review of jamming attacks in wireless systems," *Int. J. Latest Technol. Eng. Manag.*, vol. 8, no. 1, pp. 16–22, 2023.

[8] E. Bout and V. Loscri, "An adaptable module for designing jamming attacks in WiFi networks for ns-3," in *Proc. of the Int. Conf. on Modeling Analysis and Simulation of Wireless and Mobile Systems*, 2022. doi: 10.1145/3551659.3559059

[9] H. S. Obaid, "Wireless network behaviour during jamming attacks: simulation using OPNET," *J. Phys. Conf. Ser.*, vol. 1530, no. 1, pp. 1–15, 2020.

[10] X. He, "Research on computer network security based on firewall technology," *J. Phys. Conf. Ser.*, vol. 1744, no. 4, pp. 1–5, 2021.

[11] S. V. Manikanthan and T. Padmapriya, "Detection of jamming and interference attacks in wireless communication network using deep learning technique," in *Proc. of First Int. Conf. on Computing, Communication and Control System*, 2021. doi: 10.4108/eai.7-6-2021.2308599

[12] A. Maghsoudlou, L. Vermeulen, I. Poese, and O. Gasser, "Characterizing the VPN Ecosystem in the wild," in *Proc. Passive and Active Measurement Conference 2023*, 2023, pp. 1–29.

[13] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surv. & Tutorials*, vol. 24, pp. 767–809, 2021.

[14] B. Xu, M. Lu, and H. Zhang, "Multi-agent modeling and jamming-aware routing protocols for movable-jammer-affected WSNs," *Sensors*, vol. 23, #3846, 2023.

[15] M. Natkaniec and M. Bednarz, "Wireless local area networks threat detection using 1D-CNN," *Sensors*, vol. 23, #5507, 2023.

[16] S. W. Nourildean and Y. A. Mohammed, "IoT based wireless sensor network improvement against jammers using Ad-Hoc routing protocols," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 7, pp. 133–147, 2023.

[17] J. S. Mertens, A. Panebianco, A. Surudhi, N. Prabagarane, and L. Galluccio, "Network intelligence vs. jamming in underwater networks: how learning can cope with misbehavior," *Front. Commun. Networks*, vol. 4, May, 2023. doi: 10.3389/frcmn.2023.1179626

[18] M. Mosleh and Z. Saber, "Design and implementation of WLAN based zigbee for personal identification," *Eng. Technol. J.*, vol. 36, no. 8A, pp. 919–924, 2018.

[19] W. Sun, M. Choi, and S. Choi, "IEEE 802.11ah: A long range 802.11 WLAN at sub 1 GHz," *J. ICT Stand.*, vol. 1, pp. 83–108, 2013. doi: 10.13052/jicts2245-800x.125

[20] K. Pahlavan and P. Krishnamurthy, "Evolution and impact of Wi-Fi technology and applications: A historical perspective," *Int. J. Wirel. Inf. Networks*, vol. 28, no. 1, pp. 3–19, 2021.

[21] G. K. Ijemaru, I. A. Adeyanju, K. O. Olusuyi, T. J. Ofusori, E. T. Ngharamike, and A. A. Sobowale, "Security challenges of wireless communications networks: A survey," *Int. J. Appl. Eng. Res.*, vol. 13, no. 8, pp. 5680–5692, 2018.

[22] M. A. Lmater, M. Haddad, A. Karouit, and A. Haqiq, "Several jamming attacks in wireless networks: A game theory approach," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 2, pp. 36–44, 2019.

[23] S. W. Nourildean, Y. A. Mohammed, and H. A. Attallah, "Virtual local area network performance improvement using ad hoc routing protocols in a wireless network," *Computers*, vol. 12, no. 2, pp. 1–18, 2023. doi: 10.3390/computers12020028

[24] Z. Xu and J. Ni, "Research on network security of VPN technology," in *Proc. 2020 Int. Conf. on Information Science and Education*, 2020, pp. 539–542.

[25] Y. K. Sharma and C. Kaur, "The vital role of virtual private network (VPN) in making secure connection over internet world," *Int. J. Recent Technol. Eng.*, vol. 8, no. 6, pp. 2336–2339, 2020.

[26] A. T. Zamani and J. Ahmad, "Wireless LAN security: IEEE 802. 11g & VPN," vol. 4, no. 2, pp. 523–530, 2014.

[27] M. Krithikaa, M. Priyadharsini, and C. Subha, "Virtual private network – A survey," *Int. J. Trend Res. Dev.*, vol. 3, no. 1, pp. 78–81, 2016.

[28] S. Jingyao, S. Chandel, Y. Yunnan, Z. Jingji, and Z. Zhipeng, "Securing a network: How effective using firewalls and VPNs are?" *Lecture Notes in Networks and Systems*, vol. 70, 2020. https://doi.org/10.1007/978-3-030-12385-7_71

[29] R. Liu, "Firewall technology strategy analysis and application research," in *Proc. 2023 IEEE 2nd Int. Conf. on Electrical Engineering, Big Data and Algorithms, Changchun, China*, 2023, pp. 1907–1911.

[30] S. W. Nourildean and A. M. Salih, "Internet of things based wireless sensor network-WiFi coexistence in medical applications," in *Proc. f 8th Int. Engineering Conf. Towards Engineering Innovations and Sustainability*, 2022. doi: 10.1109/IEC54822.2022.9807574

[31] T. A. Khaleel, "Analysis and implementation of kerberos protocol in hybrid cloud computing environments," *Eng. Technol. J.*, vol. 39, no. 1B, pp. 41–52, 2021.

Shayma Wail Nourildean is a lecturer (a member of an academic staff) in Communication Engineering department in University of Technology (UOT), Baghdad – Iraq. She is Ph.D. student now in computer engineering in University of Tunis Al-Manar. She Holds a M.Sc. degree in Control and Computer Engineering with specialization in Computer Engineering since 2006 and she received B.Sc. degree in Computer Engineering from Baghdad University in 2002. Her research areas are Computer Networks, Data Communication and Wireless Sensor Networks. She published a number of papers in national and international journals and participated in multiple national and international conferences. She can be contacted at email: Shayma.w.nourildean@uotechnology.edu.iq.