مجلة دجلة • المجلد ٦ ،العدد ٣ (٢٠٢٣)، ص: ١٩ - ٣٠
ISSN: 2222-6583

Analyzing the Effects of VPN and Firewall Integration for WiMAX Security Using OPNET Modeler

Sabbar Insaif Jasim
Computer Technique's Engineering Department, Dijlah University College, Baghdad, Iraq.
sabar.nassif@duc.edu.iq

Abstract:

WiMAX is a wireless transmission system that provides widespread utilization of the fast internet. Securing WiMAX networks is important to protect against a range of threats such as eavesdropping, jamming, and unauthorized access. Various security protocols have been introduced. One such protocol is Virtual Private Network (VPN), which leverages Data Encryption Standard (DES) to secure data transmission.This paper examines This paper examines the impact of integrating VPN with firewall to secure WiMAX, using OPNET Modeler (v14.5) as the simulation tool. The study focuses on four applications, namely Email, web browsing, file transfer, and database. Results of the simulation show that the existence of VPN reduces the amount of data transmitted per second. Firewall, on the other hand, blocks web browsing access from the server. However, the VPN enables selective access to the web browsing application from a specific source, i.e., Base Station1. The advantage of integrating a VPN towards the system is that it increases system security because no client from any base station may access any server application.

Keywords: WiMAX, Firewall, Server, Security, Ethernet

Introduction

WiMAX is a requirement wireless system that enables users to access the internet and other multimedia services at extremely fast speeds. Local area network (LAN) continues to be used by Wi - fi technology in the foreseeable future [1]. The distinctions between wifi and WiMAX are as follows.

Cost, speed, distance, and other factors are the main differences between WiMAX technology and Wi-Fi technology. The range of WiMAX is around 30 miles, while that of Wi-Fi is relatively constrained to a narrow area. WiMax network functions as an ISP without the usage of cables because WiMAX networks are used to deliver internet access to your house or place of business, whereas Wi-Fi is used internally within local area networks (LANs) to access the internet [2].

Metropolitan area networking (MAN) is made possible by the WiMax architecture. WiMax's base station may provide access to businesses and hundreds of residences, whereas Wi-Fi only offers local area networking (LAN) [3].

Wireless systems always make some people worried when speaking of security. The integration of VPN (Virtual Private Network) with a firewall for securing WiMAX (Worldwide Interoperability for Microwave Access) is a powerful combination of technologies that can provide improved security and performance for wireless networks and give several solutions.

To evaluate the effects of combining a VPN and firewall for protecting WiMAX, this study makes use of OPNET Simulator., a network simulation tool. The simulation runs four WiMAX applications to analyze the impact of integrating VPN and Firewall on data transmission. The four applications studied are Email, web browsing, file transfer, and database. The results of the simulation provide valuable insights into the effectiveness of the integration of VPN and Firewall for securing WiMAX. The findings of the study show that the integration of VPN and Firewall can reduce the number of bits transmitted per second, which is a trade-off for the increased security provided. Additionally, Firewall blocks all web browsing access from the server, while the VPN allows selective access to web browsing from a specific source. This selective access is more secure than allowing access from any base station to any server application [4-9].

WIMAX

A wireless communication technique called WiMAX (Worldwide Interoperability for Microwave Access) offers widespread high-speed connection to the internet. It is based on the IEEE 802.16 standards and employs wireless signals instead of cables or wires to carry data across large distances, up to several miles or kilometers [10-14]

Broadband internet service can be provided using WiMAX in remote or rural locations where traditional wired connections are not practical or practical. It can also be utilized to give users who are travelling inside a WiMAX service area access to mobile internet. Voice over IP (VoIP), teleconferencing, and information in any manner are just a few of the applications that WiMAX can enable [15-18], [2],. WiMAX can run in both licensed and unlicensed frequency areas. Compared to other wireless devices like Wi-Fi and cellular networks, WiMAX has a variety of benefits. Higher data transmission rates, a larger service area, and improved network security are all provided[19-22]. Unfortunately, it has not been as widely adopted as other wireless technologies, and 4G and 5G cellular networks have essentially taken its position as the primary means of mobile internet access [23-26].

Related Work

In 2022, Shayma W. Nourildean, Siddeeq Y. Ameen, And Yousra A. Mohammed used OPNET modeler, a good tool for simulation wimax networks, to examine the effect of VPN and firewall to protect wimax [27]. Ammar O. Barznji And Jalal J. Hamad Ameen assessed signal coverage in a designated area to determine data capacity with minimal delay in October 2021, using WiMAX network design and analysis. [28]. The workings and effectiveness of firewalls and VPNs, including their technologies and benefits, as well as addressing security flaws, potential risks and proposing solutions were explained By Sun Jingyao, Sonali Chandel, Yu Yunnan, Zang Jingji, And Zhang Zhipeng, 2020 [29].

In 2019, Nidhi Lal And Shishupal Kumar suggested a secure uplink scheduler for the WiMax mac layer. it uses a heuristic approach for scheduling and includes authorization procedures to prevent security attacks like dos and flooding attacks, securing the allocation of bandwidth from malicious nodes.[30].

Simulation Setup

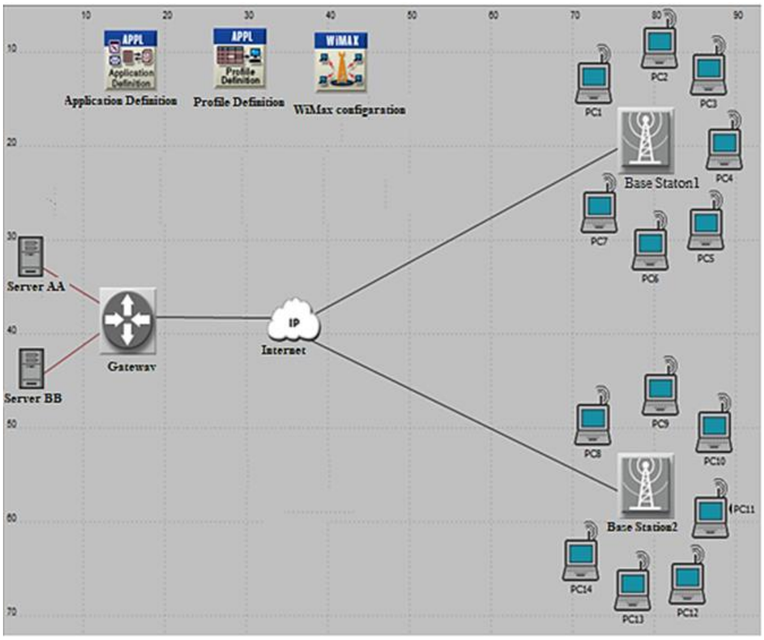
OPNET was chosen as the essential instrument for modeling the WiMAX system in this investigation. A dynamically, occurrence framework emulator called OPNET can effectively and precisely mimic the behavior of real networks. It is a creation of OPNET Technologies Inc. and is utilized frequently by specialists, businesses, and academics. WiMAX, WLAN, LAN models, as well as other systems can be simulated by OPNET. [31],[32].

The simulator setup used by OPNET consists of a variety of scenarios, each of which includes a variety of items that connect with one another via different programs like mails, file transfers over FTP, web surfing over HTTP, and database systems. The following situations were employed:

4.1. Case 1: No VPN and no Firewall

In this case, WiMax without VPN or firewall was simulated by the estimated network. The following objects were part of the network's topology:

- Application definition: describing the network application
- To define the profile of the application for the network, use a profile.
- WiMAX configuration: setting up WiMax supporter stations and network stations.
- WiMAX BS ethernet4 slip4 router stations: Server - Ethernet Server Base.
- Ethernet4 slip8 gtwy is the gateway
- Internet - IP Cloud Links: All links except the one from the Ethernet server to the gateways are PPP DS3.



Fig/ 1. Case 1 (Network without a Firewall or VPN)

4.2. Case 1: Firewall without VPN

The system in Scenario 2 is modeled after WiMAX architecture and has a firewall but no VPN. The important components make up the topology of the network:

- Identification of an application: used to define which applications are permitted to execute on a system.
- WiMAX configuration is used to build up the WiMAx networking.
- Platforms are WiMAX subscription units.
- Profile definition is used to establish the characteristics for the communication networks.
- Base stations: WiMAX BS ethernet4 slip4 router; Server: Ethernet server
- Ethernet4 slip8 gtwy is the gateway.
- Firewall: ethernet2 slip8 firewall;
- Internet: IP Cloud

- Links: These are the network links' configurations: All other links are PPP DS3, except for the 100BaseT connection between the Ethernet server and the gateway.
- Fig.2. explain Case 2 (Network with Firewall and no-VPN)
- In this case, firewalls shield servers from every unauthorized access to the server AA's HTTP web surfing application.

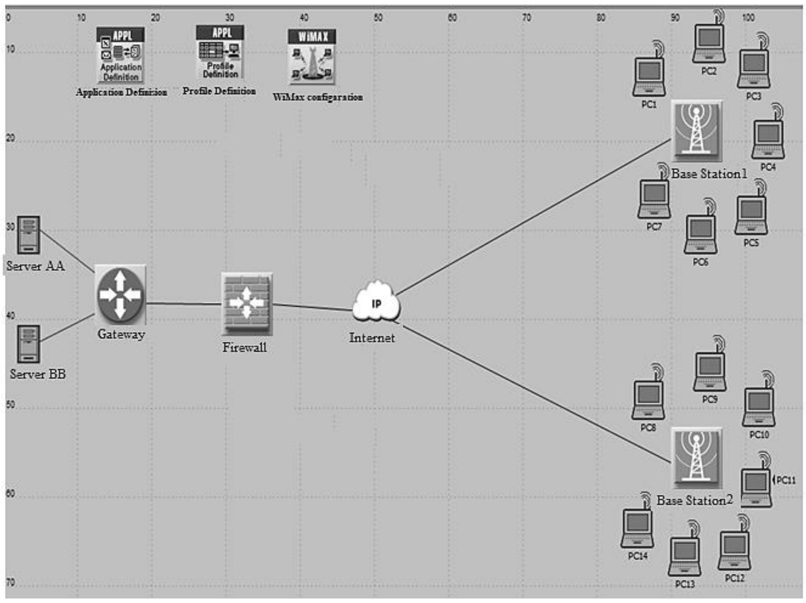


Fig.2. Network with Firewall and no-VPN

4.3. Case 3 : VPN and Firewall

In case 3, a system featuring WiMAX technology with both a firewall and a VPN is modeled. The essential elements make up the network topology as in fig.3:

- Application definition: describing the network application
- To define the profile of the application for the network, use a profile.
- WiMAX Configuration: Network WiMax configuration
- VPN Config.: WiMAX subscriber stations for VPN configuration
- Ethernet server base stations for servers -WiMAX BS ethernet4 slip4 router
- Ethernet4 slip8 gtwy is the gateway
- Ethernet2 slip8 firewall,
- Internet-based IP Cloud Firewall
- Links: 100BaseT from the Ethernet server to the gateway; PPP DS3 for all other links.

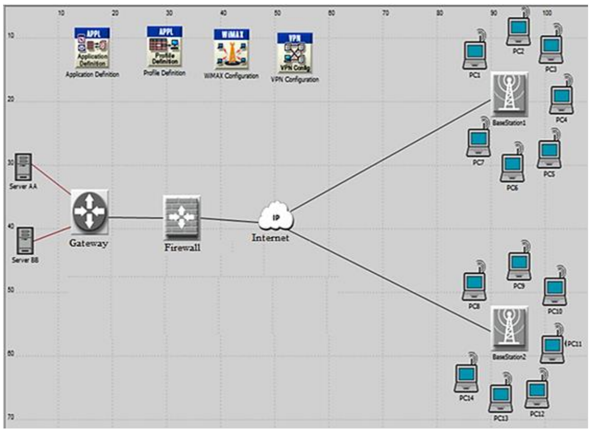


Fig.3. Case 3 (Network with Firewall and VPN)

In this case, the VPN connection would serve to enable one of BaseStation1's customers (PCs) to connect to Server AA and use the HTTP application for online browsing. Due to IP packets in the tunnel being contained inside IP datagrams, the BaseStation1 traffic will not be blocked by the firewall.

Following the configuration of the three situations (No Firewall No VPN, Firewall No VPN, and Firewall VPN), DES (Discrete Event Statistics) were selected for these cases to examine the system's performance in terms of a few criteria for email and web surfing (HTTP) applications. The simulation was performed for 30 minutes with the number of statistics for each scenario selected, and the results were compiled as shown in the next section.

Results and Discussion

5.1. Throughput

It defined as the average number of bits transmitted in the network per second, differed for the three scenarios

- No firewall - no - VPN
- Firewall - no - VPN
- Firewall with VPN

The values recorded were 704,470.4 bits/sec, 722,382.9 bits/sec, and 668,668.3 bits/sec, respectively. The network's throughput was lower when a firewall and VPN were integrated, which can be attributed to the fact that the VPN with firewall restricts server access, as indicated in the findings shown in fig. 4. Therefore, the findings imply that although the combination of firewall and VPN may enhance network security, it may potentially compromise network performance as evidenced by the decreased throughput in the Firewall with VPN scenario.

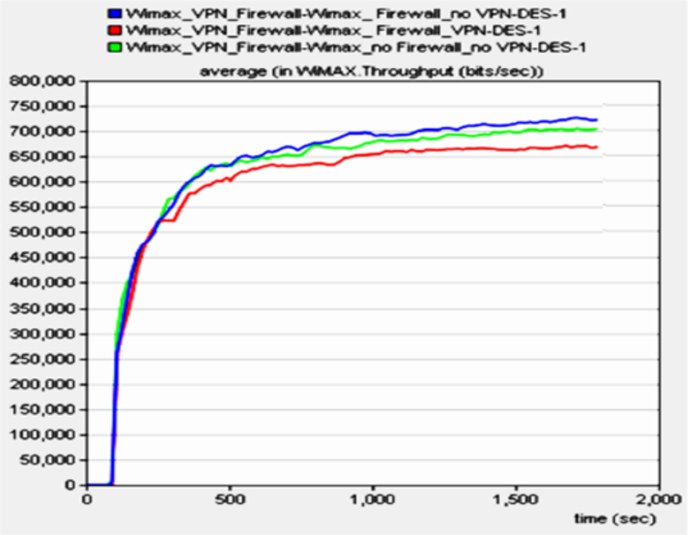


Fig.4 Three scenarios for WiMax throughput

5.2. The Delay

The delay, the end-to-end latency of all information carried by all WiMax MACs in the system and transmitted to the higher layer, known as the delay, was roughly the same for all three situations.

- No firewall – no VPN
- firewall - no VPN
- firewall - VPN

Unless for the no firewall – no VPN is scenario which had a larger delay.

The delay in the (No Firewall- No VPN) scenario reached 0.085 sec at the start of the simulation period (108 sec), whereas the delay in the other two scenarios stayed at a level lower. But, as the simulation went on, the (No Firewall No VPN) scenario's latency shrank and caught up to the others as shown in fig.5.

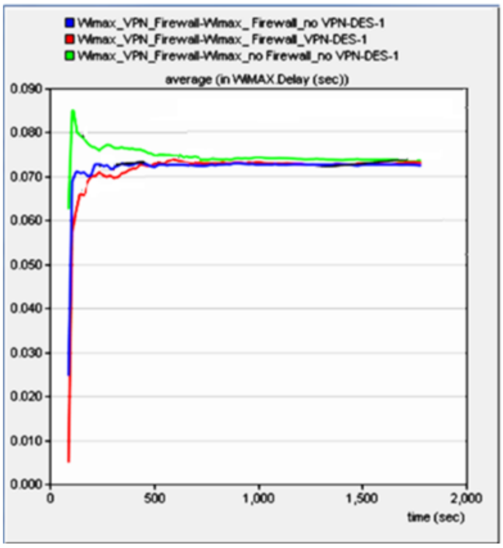


Fig.5 WiMAX Delay for three scenarios

Despite the firewall, there was some traffic sent and received over the network through VPN since it was necessary to use a VPN connection to enable one of BaseStation1's customers (PCs) to reach Server AA for an HTTP application. Due to IP packets in the tunnel being contained within IP datagrams, the BaseStation1 activity will not be blocked by the firewall.
Data Encryption Standard (DES) was employed to investigate the impact of VPN on individual nodes in the WiMAX system. The effectives are as shown below:

The analysis focused on the traffic received and sent for HTTP application on Server AA, which was represented in Fig. 6 and Fig. 7, respectively. It was observed that in the network with firewall and without VPN, no traffic was sent or received. This was due to the fact that the firewall blocked all HTTP access to Server AA. On the other hand, in the network without firewall and VPN, there was a high amount of traffic sent and received. This was because there were no restrictions or limitations on the network, and all the clients could access Server AA for HTTP application.

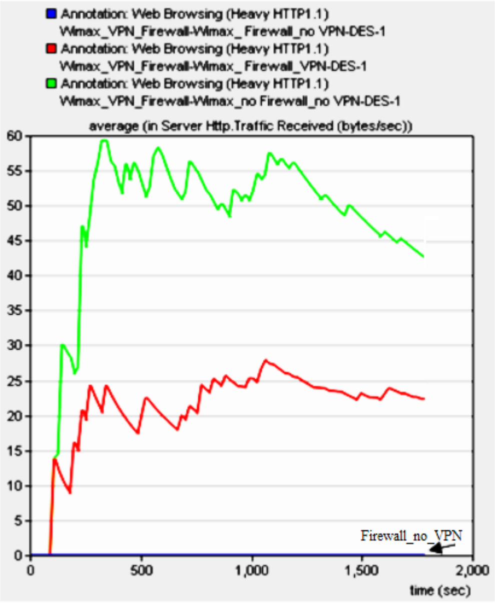


Fig.6 Traffic Received for three scenarios with HTTP (Web browsing) Application

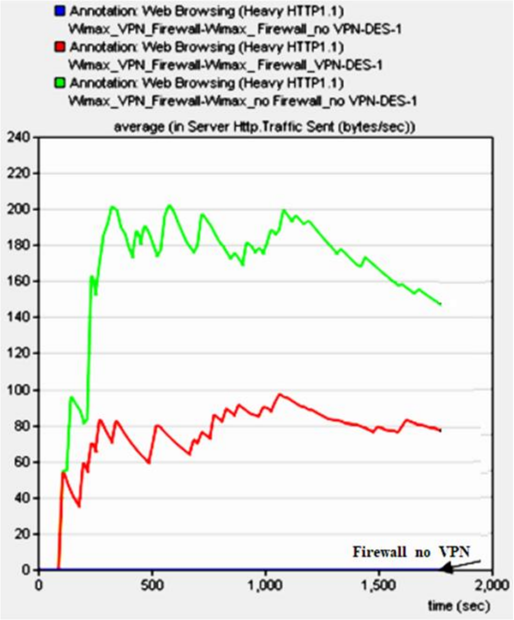


Fig.7 Traffic Sent for three scenarios with HTTP (Web browsing) Application

However, in the network with VPN, even with the presence of the firewall, there was some traffic sent and received. These occurred as a result of one of the customers (PCs) from BaseStation1 (BS1) being able to connect to Server AA through a VPN tunnel. Due to IP packets in the tunnel being wrapped inside IP datagrams, the BaseStation1 traffic will not be blocked by the firewall.

Overall, the study demonstrated that VPN is a useful tool that can be used to bypass firewalls and enable clients to access resources that would otherwise be inaccessible. By maximizing the use of VPN, the study's findings can be leveraged to enhance the security and functionality of WiMax systems.

Figures 10 and 11 display the traffic sent and received on Server AA for the Email application under three different scenarios, namely (no Firewall * no VPN), (Firewall * no VPN), and (Firewall with VPN). It can be observed from the figures that there was traffic sent and received in all the scenarios. This is because the firewall only protects Server AA from web browsing (HTTP) access and not from Email access.

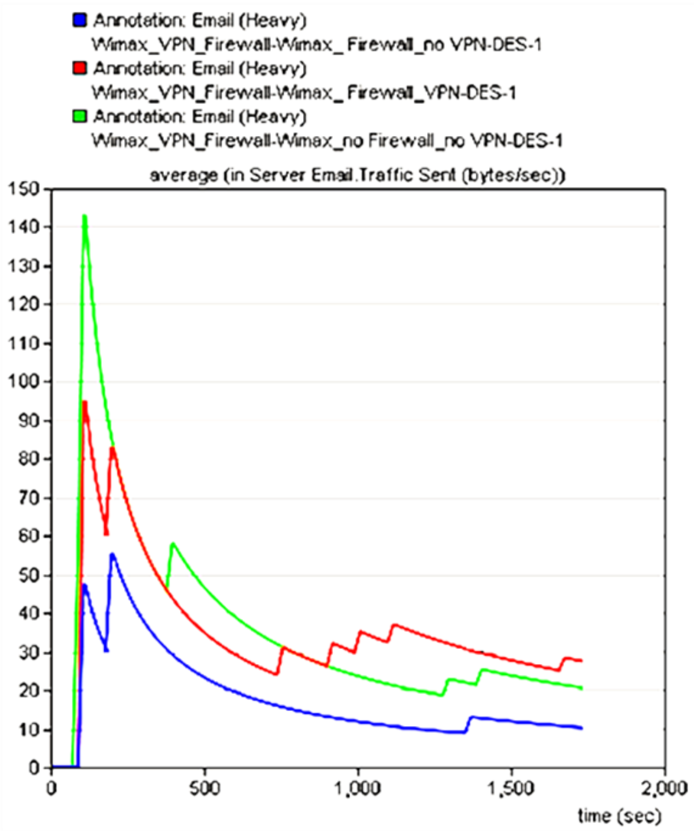


Fig. 10 Traffic Received for three scenarios Email Application

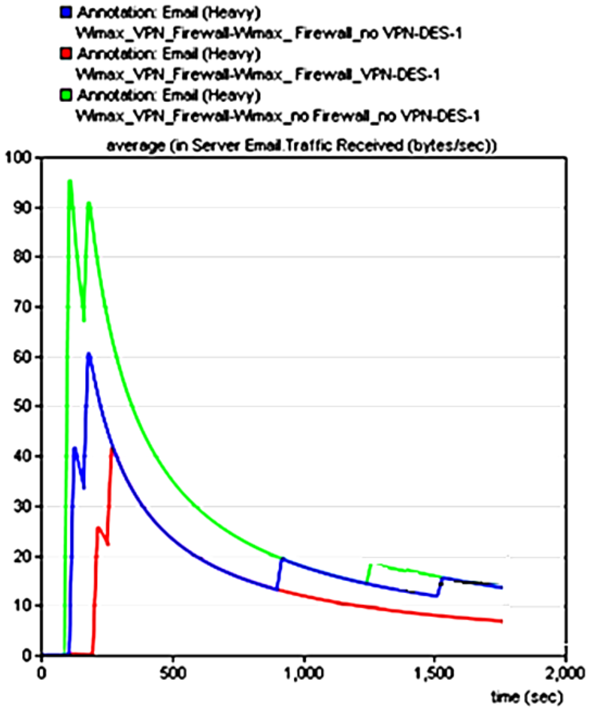


Fig.11. Traffic Sent for three scenarios with Email Application

Conclusion

This study highlighted the value of security in WiMAX and presented WiMAX, a newer technique. The study looked at how a firewall affected four applications when it was combined with a private Virtual Private Network (VPN) to increase WiMAX security (Email, HTTP, FTP, and Database). The findings demonstrated that the firewall without a VPN protected the server from network HTTP access. When incorporated into the system, the VPN concurrently screened packets for HTTP access from a certain source to a particular destination. This was accomplished by enabling one of BaseStation1's clients to access HTTP from server AA through a VPN connection.

The IP datagram will contain the IP packets in the tunnel. Therefore the firewall will not be able to filter the traffic of BaseStation1 over the tunnel. Through the deployment of VPN technology, WiMAX was made secure while also reducing system traffic by enabling only certain users and sources to connect to the server. The study only looked at one server, but looking at many servers would produce findings that would show how useful VPNs are for connecting particular clients to particular servers. Because it allowed for the measurement of numerous characteristics, including throughput, delay, and traffic delivered and received, OPNET was a suitable instrument for this investigation.

Overall, the study demonstrated that VPN is a useful tool that can be used to bypass firewalls and enable clients to access resources that would otherwise be inaccessible. The study's findings can be used to enhance the performance and security of WiMAX systems by optimizing the use of VPN

rovide a statement that what is expected, as stated in the "Introduction" chapter can ultimately result in "Results and Discussion" chapter, so there is compatibility. Moreover, the prospect of the development of research results and application prospects of further studies can also be added into the next (based on result and discussion).

References

[1] Chandan , R. K. Ratnesh, and Amit Kumar. "A compact dual rectangular slot monopole antenna for WLAN/WiMAX applications", In Innovations in Cyber Physical Systems: Select Proceedings of ICICPS 2020, Springer Singapore, 2021, pp. 699-705.

[2] S. A. Ahson and M. Ilyas, 2018," WiMAX: technologies, performance analysis, and QoS. CRC press". 2018 Oct 8. CRC press, books.google.com.

[3] Abdellah Attalhaoui1 and *et al*, "Design of agile monopole antenna for WiFi and WiMAX applications", 2022, E3S Web of Conferences *351*, 01081, ICIES’22, 2022, https://doi.org/10.1051/e3sconf/202235101081,

[4] Anwar, Raja Waseem, Tariq Abdullah, and Flavio Pastore. "Firewall best practices for securing smart healthcare environment: A review.", Applied Sciences, 2021,11, no. 19 pp: 9183.

[5] Sultana, Rukhsar, Jyoti Grover, and Meenakshi Tripathi. "Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges.", Vehicular Communications, 2021, 27: pp100284.

[6] Iqbal, Muhammad, and Imam Riadi. "Analysis of security virtual private network (VPN) using openVPN.", International Journal of Cyber-Security and Digital Forensics1, 2019, 8, no.: pp.58-65.

[7] Lal, Nidhi, and Shishupal Kumar. "An Efficient Uplink Scheduler for WiMAX Communication System with Prevention from Security Attacks.", New Review of Information Networking, 2019, 24, no. 2: pp133-152.

[8] Bashiri, Maryam, Changiz Ghobadi, Javad Nourinia, and Maryam Majidzadeh. "WiMAX, WLAN, and X-band filtering mechanism: Simple-structured triple-band frequency selective surface.", IEEE Antennas and Wireless Propagation Letters 16 2017:pp 3245-3248.

[9] Jeyapoornima, B., J. Joselin Jeya Sheela, C. Malarvizhi, S. Vanaja, Rahul Krishnan, and Rajasekhar Atla. "Multi-band narrow strip antenna for 5G/WLAN/WiMAX Wireless Communication." International Conference on Computer Communication and Informatics (ICCCI), 2021 pp. 1-4. IEEE.

[10] Song, Shuang, and Biju Issac. "Analysis of WiFi and WiMax and wireless network coexistence." 2014, arXiv preprint arXiv:pp1412.0721

[11] Murty, M. Sreerama, A. Veeraiah, and Srinivas Rao. "Performance evaluation of Wi-Fi comparison with WiMax networks.", 2012, arXiv preprint arXiv:pp1202.2634 .

[12] Litake, Shilpa, and Prachi Mukherji. "SFP-based vertical handover with MIH services for integrated Wi-Fi and WIMAX networks." International Journal of Mobile Network Design and Innovation 9, no. 2, 2019: pp85-96.

[13] Sekkal, Soukaina, Laurent Canale, and Adel Asselman. "Flexible textile antenna design with transparent conductive fabric integrated in OLED for WiMAX wireless communication systems.", 2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), pp. 1-4. IEEE.

[14] Ullah and *et al*, "Super wide band, defected ground structure (DGS), and stepped meander line antenna for WLAN/ISM/WiMAX/UWB and other wireless communication applications.", Sensors 20, 2020, no. 6: pp1735.

[15] Alsharbaty, Firas, and Qutaiba I. Ali. "A Cybersecurity Model for the Enhancement of WiMAX-based Wireless Communications Infrastructure to Serve Smart Grid Applications.", International Journal of Smart Grid-ijSmartGrid 7, 2023, no. 1 pp: 15-24.

[16] Alghannam, AHMED I., and A. K. Alhafid. "Performance analysis of Unsolicited Grant Service (UGS) service class in WiMAX VoIP application.", J. Eng. Sci. Technol 15, 2020, no. 3 pp: 1481-1491.

[17] Alfaisaly, Noor Nateq, Suhad Qasim Naeem, and Eman K. Jassim. "The Effect of Different Mobile Trajectory on the Performance of VoIP Application in WiMAX Network." 2022 9th International Conference on Electrical and Electronics Engineering (ICEEE), pp. 141-146. IEEE, 2022.

[18] Lawal, Ibrahim A. "A New Distributed Model Comparison to Enhance VoIP QoS Performance over WLAN and WiMAX Network.", Ilorin Journal of Computer Science and Information Technology 3, 2020, no. 1,: pp11-22.

[19] Mohammad Saadh, A. W., Shashank Khangarot, B. V. Sravan, Namratha Aluru, Poonkuzhali Ramaswamy, Tanweer Ali, and Manohara MM Pai. "A compact four-element MIMO antenna for WLAN/WiMAX/satellite applications.", International Journal of Communication Systems, 2020, 33, no. 14 : e4506.

[20] Simarata, J. H. T., and S. Suherman. "Downlink ratio impact on downstream traffic performances on WiMAX.", In IOP Conference Series: Materials Science and Engineering, 2020, vol. 725, no. 1, pp. 012057. IOP Publishing,.

[21] Abdalgader, Khaled, and Dinesh Kumar Saini. "Data Streams Scheduling Approach for WiMAX Networks Journal of Communications Vol. 15, No. 6, June 2020, pp 469-479.

[22] Bandhu, Kailash Chandra, and Ashok Bhansali. "Comparison of Transmission Control Protocol Variants for Two Way Transfer and Propagation Model with WiMAX Network Bandwidth Asymmetry.", 2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE) , 2020, pp. 1-5. IEEE.

[23] Hajlaoui, Emna, Aida Zaier, Abdelhakim Khlifi, Jihed Ghodhbane, Mouna Ben Hamed, and Lassâad Sbita. "4G and 5G technologies: A Comparative Study." In 2020 5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), 2020, pp. 1-6. IEEE,.

[24] Victor-Ikoh, Maudlyn I., and Anasuodei Moko. "Fixed Wireless Access: An Explorative Study of WIMAX FWA and 5G FWA Networks.", International Journal of Computer Science and Mobile Computing, Vol.10 Issue.4, April- 2021, pp. 99-107.

[25] Alezabi et al. . "Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks.", EURASIP Journal on Wireless Communications and Networking", 2020:1052020, no. 1,pp 1-34. https://doi.org/10.1186/s13638-020-01702-8.

[26] Benalia, Elhadja, Salim Bitam, and Abdelhamid Mellouk. "Data dissemination for Internet of vehicle based on 5G communications: A survey.", Transactions on Emerging Telecommunications Technologies 31, 2020,no. 5: e3881. Volume31, Issue5 Special Issue: Future Internet of Vehicles May 2020

[27] Nourildean, Shayma W., Siddeeq Y. Ameen, and Yousra A. Mohammed. "VPN–Based WiMAX Network Protection Against Jamming Attacks for VoIP Application.", Journal of Physics: Conference Series, vol. 2312, no. 1, pp. 012065. IOP Publishing, 2022. DOI: 10.1088/1742-6596/2312/1/012065.

[28] Barznji, Ammar, and Jalal Ameen. "Wi-Max Network Simulation For Salahaddin University New Campus.", Kufa Journal of Engineering 12, 2021, no. 4 pp 1-13.

[29] Jingyao, Sun, Sonali Chandel, Yu Yunnan, Zang Jingji, and Zhang Zhipeng. "Securing a network: how effective using firewalls and VPNs are?.", In Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Springer International Publishing, 2020. Volume 2, pp. 1050-1068

[30] Lal, Nidhi, and Shishupal Kumar. "An Efficient Uplink Scheduler for WiMAX Communication System with Prevention from Security Attacks." New Review of Information Networking 24, 2019, no. 2 pp 133-152.

[31] Alfaisaly, Noor Nateq, Suhad Qasim Naeem, and Azhar Hussein Neama. "Enhancement of WiMAX networks using OPNET modeler platform.", Indonesian Journal of Electrical Engineering and Computer Science 23, 2021, no. 3 pp: 1510-1519.

[32] Abdulrazzaq, Ali Abdulwahhab, Ahmed Jabbar Abid, and Adnan Hussein Ali. "QoS performances evaluation for mobile WIMAX networks based on OPNET.", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 9 (2018) pp. 6545-6550.