Wireless Networks Encryption by Simulation of Attacks

Iyas Alodat
Faculty of Computer Science and Information Technology, Jerash University, Jerash, Jordan
Email: eyas.odat@jpu.edu.jo

***Abstract*—Wireless LANs widespread use is attributable to a combination of factors, including simple construction, employee convenience, connection selection convenience, and the ability to support continual movement from residences to large corporate networks. For organizations, however, the availability of wireless LAN means an increased danger of cyberattacks and challenges, according to IT professionals and security specialists. This paper examines many of the security concerns and vulnerabilities associated with the IEEE 802.11 Wireless LAN encryption standard, as well as typical cyber threats and attacks affecting wireless LAN systems in homes and organizations, and provides general perception of weaknesses for home and business users.**

***Index Terms*—cyber-attack, IEEE 802.11, encryption, TCP&UDP, OMNET++**

I. Introduction

WLAN is the most widely recognized wireless broadband technology capable of high transmission rates; Wi-Fi allows users to access the Internet without using cables from anywhere. The Omnet++ tool is used to coordinate the operation of a group of Access Points (APs) [1], each supporting a distinct WLAN technology standard, which are deployed to provide a variety of applications, for multiple WLAN standards like (802.11b, infrared, 802.11 frequency hopping) [2]. We discussed the various metrics, such as WLAN load, WLAN delay, WLAN throughput, media latency, TCP churn, and queue size through simulation.

Wi-Fi stands for "Wireless Fidelity." Wi-Fi is an alias for IEEE 802.11 Wireless Personal Area Network (WLAN), a technology that allows electronic devices to connect to a wireless network, particularly those that adopt the 2.4GHz and 5GHz radio bands. Wi-Fi is a WLAN communication technology that is segmented into various IEEE 802.11 standards and described by extensions. The 802.11 standard describes numerous physical layers and characteristics of Wi-Fi technologies. VHT (Very High Throughput) is the most recent new physical layer, and it is described in an upgrade to the IEEE 802.11ac standard. Emulation, coding systems, and debugging are all tasks that PHY is in charge of [3].

802.11 Wireless LAN has evolved and altered the entire network landscape in recent years. Ethernet is being phased out in favor of 802.11n [4]. It is the network method that allows for the rapid deployment of mobile devices, particularly in locations where there is a high demand for WLAN, such as homes, educational institutions, commercial and government offices, airports, buildings, military facilities, cafes, libraries, and other locations. WLAN also draws the majority of mobile wireless devices to companies and consumers all over the world due to its ease and flexibility. Anyone with a basic understanding of computer networking may set up their own wireless network using the low-cost, easy-to-use installation methods and equipment.

However, as wireless networks have grown in size as a result of improvements in technology, the threats have increased for home users and small enterprises, as well as major corporations. A WLAN uses radio waves to communicate. As a result, all network users in the first and second layers would be exposed to radio frequency listening, which is one of the most significant security vulnerabilities [5]. IEEE standard security for wireless networks is one of the most serious security weaknesses. The 802.11i standard, also known as Wi-Fi Protected Access (WPA) [3], was established by the Wi-Fi Alliance to address serious security weaknesses in the WEP standard.

In this paper there will be an examination of the two types of network protocols, TCP and UDP. This is required to determine potential weaknesses. And after that, we will examine the methods that can be used to deal with these challenges in important to deter intrusion into the network and obtain critical information from it.

II. Related Work

A lot of work have demonstrated the IEEE 802.11i standard which does not protect against eavesdropping and different denial-of-service attacks, such as electronic authentication and disengagement cyberattacks [6], [7]. Furthermore, the flexibility and backward compatibility of WEP's 802.11i pre-shared key placement allowed using a vocabulary and brute force cyberattacks easier for most hackers [8]. Experiments also found that fewer of Wi-Fi networks were discovered using the outdated WEP encryption protocol, which has already been proven to be broken in a little over a second using freely available hacking tools [9]. As a result, wireless LAN security remains a major problem in both residential and business networks.

Manuscript received February 28, 2022; revised April 11, 2022; accepted April 14, 2022.
Corresponding author: Iyas Alodat (email: eyas.odat@jpu.edu.jo).

doi: 10.18178/ijeetc.11.5.351-355

Along with their flexibility, efficiency, simplicity of access, installation, and cost savings, wirelesses LANs have surpassed conventional networks, like video application [10]. However, as a result of this expansion, wireless networks will face more vulnerabilities and difficulties in terms of attacker targeting and the possibilities of this work [11]. To transfer data over the air, wireless networks employ radio or infrared beams. Wireless networks have a large monitoring range within which an attacker may monitor the network, which endanger the data's integrity. In the face of this space of sabotage for attackers, protecting the wireless network is a big issue for IT security practitioners and system administrators [12]-[16].

This paper outlines the IEEE 802.11 security standard's weaknesses as a security concern, as well as the primary known attacks/threats to residential and corporate wireless LAN systems. The remainder of the paper is structured as follows: Section II contains relevant work. In Section III, we will take a quick look at WLANs. Section IV discusses common vulnerabilities and security issues associated with the IEEE 802.11 security standard and WLAN. Following that, a thorough examination of prevalent WLAN risks and cyberattacks is provided. Section VI and Section VIII contain a discussion about the emulator and an examination of the recommendations, as well as an overall recommendation, whereas Section VIII contains the conclusion.

III. IEEE 802.11 and Advancement

IEEE defines and implements a variety of protocols for the electrical and computer sectors, such as Wi-Fi 802.11, Ethernet, and IEEE 802.3. The IEEE presently has over 1,100 commercial standards in use, with another 600 in the development. IEEE 802 LANs are one of the most well-known standards, while IEEE 802.11 is among the most common [17]-[19].

A. IEEE 802 Standard

All Wi-Fi systems for multiple geographical areas networking (LAN/MAN) are covered under the IEEE 802 standard. The IEEE 802.11 series is responsible for Wi-Fi protocols.

A suffix letter was not included in the initial Wi-Fi standard, which was issued in 1997. When further variants were produced, however, a suffix letter was added to identify the actual variant. This was a lowercase letter.

B. 802.11A Standard

This standard was the first in the 802.11 series of Wi-Fi technologies. A wireless carrier was suggested using orthogonal frequency division multiplexing in the ISM 5 GHz band with data rates of up to 54 Mbps [20].

802.11a was exactly as popular as 802.11b, despite its widespread use. Although the 5GHz band was actually larger and could handle more channels, it was more costly at the time, limiting its adoption.

C. Standard 802.11B

It has considerably more widespread adoption than the 11a standard. Although the highest raw data rates were just 11 Mbps, the standard utilized the 2.4 GHz ISM band, which was cheaper at the time. Furthermore, Wi-Fi usage was vastly smaller during time, and interference was not as widespread as it is now.

D. Standard 802.11G

The 802.11b standard was developed in response to the need for faster 2.4 GHz Wi-Fi. 802.11g achieves raw data transmission rates of 54 Mbps by using OFDM technology.

It is also a DSSS available digitally, meaning it could communicate at the slower 802.11b rate. Backwards compatibility was necessary because of the large number of outdated access points and PCs that may only support the previous standard, so it is a challenge.

IV. WLAN Vulnerabilities

Wireless LANs have exceeded conventional networks in popularity with high flexibility, cost-effectiveness, and ease of installation. However, as WLANs have grown in popularity, the hacker's possibilities have expanded. WLANs, unlike wired networks, deliver data over the air via radio frequency or infrared transmission.

An attacker may monitor a wireless connection and, in the worst-case scenario, compromise data integrity using current wireless technologies. When it comes to securing a WLAN, there are several security considerations that IT security practitioners and system administrators must address [21].

With 802.11 networks, radio frequency interference is a major concern. The majority of wireless LAN protocols, as well as the other devices such as Bluetooth, wireless phones, and microwave broadcasts, use the 2.4GHz channel frequency range. This can cause signal interference and the termination of a valid user [22], [23].

WLANs suffer a distinct set of vulnerabilities than cable LANs due to their inability to properly restrict radio waves. Even if businesses set up their own access points and use antennas to guide their signals in a certain direction, it is impossible to entirely prevent wireless broadcasts from reaching undesired locations like nearby lobbies, semi-public areas, and parking lots. As a result, hackers will have easier time obtaining sensitive information [23], [24].

V. WLAN General Attacks/Threats

An attack is an activity taken by an intruder in attempt to compromise the organization's information. Wireless local area networks (WLANs), unlike wired networks; communicate via radio frequency or infrared transmission technologies, rendering them open to cyberattack. These attacks are designed to compromise information confidentiality, integrity, and network availability. As shown in Fig. 1, the following are the two types of man-in the middle attacks:

- Negative attacks.
- Active attacks.

Both negative and passive attacks are ones in which the attacker attempts to get information sent or received by the network. Because the attacker does not alter the

contents of the file, these cyberattacks are generally difficult to detect [25]-[27]. Traffic analysis and mottling are the two forms of passive attacks [28].

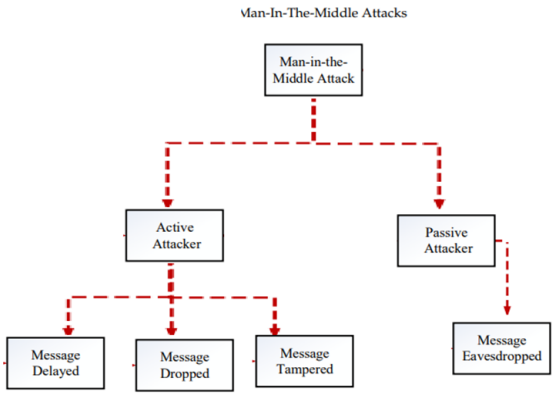

Fig. 1. Man-in the middle attacks.

In Active cyberattacks, on the other hand, the attacker not only obtains access to the network's data, but also actively alters or produces fake data on the network. Any business will incur a considerable loss as a result of such nefarious behavior [9].

VI. Emulator Environment

We scanned the network through the use of the Omnet++ program, which is linked to the NETA and INET platforms, and through them we created a simulated network for the network to be examined. The shape of the network to be examined is of the type IEEE 802, and the network consists of 20 broadcast points that are normal and a variable number of attacking points that we will specify while running the emulator. All these normal and attack points will be connected to a single network within a specific geographical range as in Fig. 2.

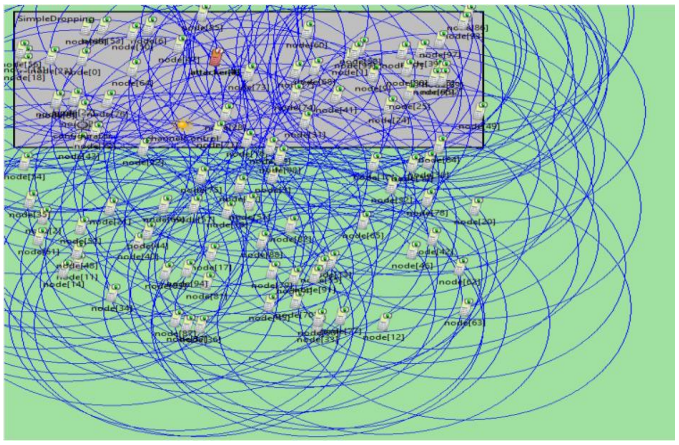

Fig. 2. Network environment; Omnet++ Network with NETA scenario.

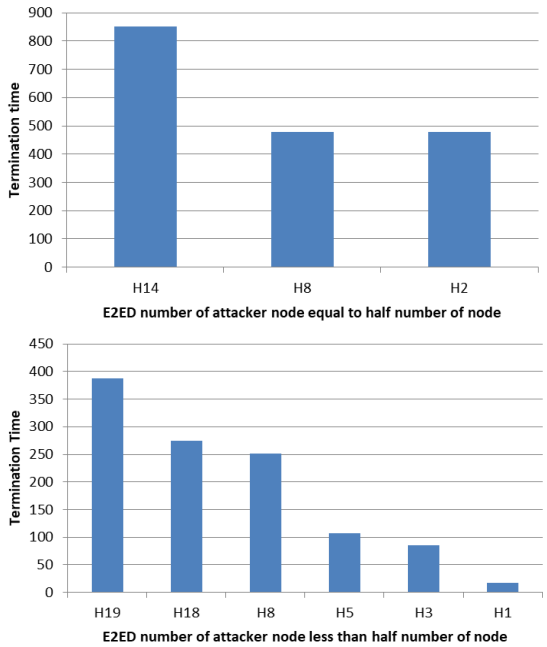

Fig. 3. The value of the termination between E2ED.

VII. Examination Process

The number of repetitions in one scenario is thirty times, for each scenario there is a change in the number of attacking points, which is {5, 10} meaning a quarter, half of the number of points in the scenario. There is also a variable in each scenario, which is the number of dropped messages, which were set at 0.1, 0.4 and 0.8 for each scenario. Thus, the total number of completed trials is 9 for each protocol {UDP, TCP}.

A. Results When Using the UDP Protocol

Firstly we will present UDP scenario. The time between the ends that the packet takes when transmitting over the network, and this time is determined by factors in terms of propagation time, transmission time, and finally processing time, in addition to the number of routers.

We notice from the Fig. 3 the value of the termination time has increased with the increase in the number of attacker nodes (E2ED) in the network, and that the number of points has also increased with the increase in the number of attackers. Therefore, the network will become more difficult to spread and process data between nodes, due to service interruption.

The number of messages that were received correctly without errors, as shown in Fig. 4, called the CDR, is a ratio that constitutes the total number of those messages over the number of messages expected to be sent in the network. Through the following figure, we can see that ratio between the two networks that were examined.

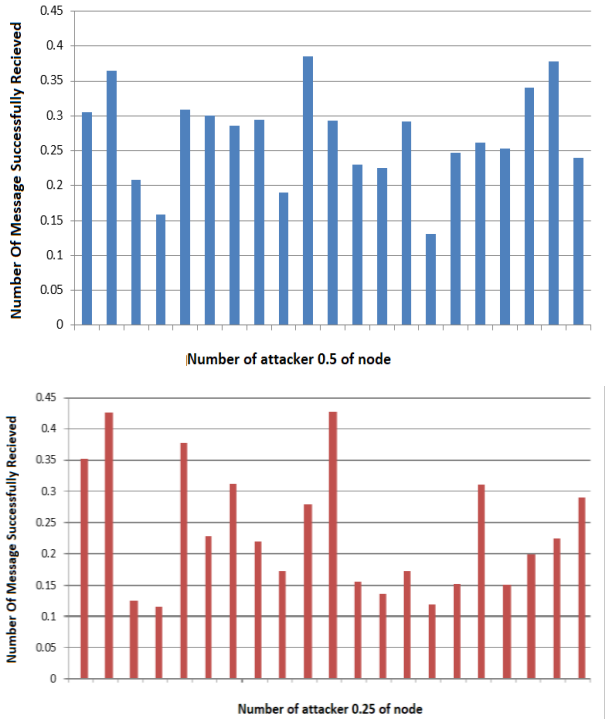

Fig. 4: CDR; message received correctly without errors.

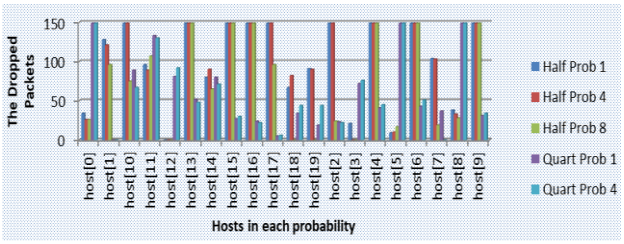

Fig. 5. The dropped packets.

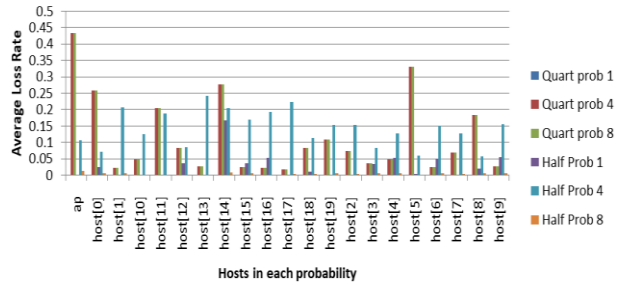

Fig. 6. Average loss rate in TCP network.

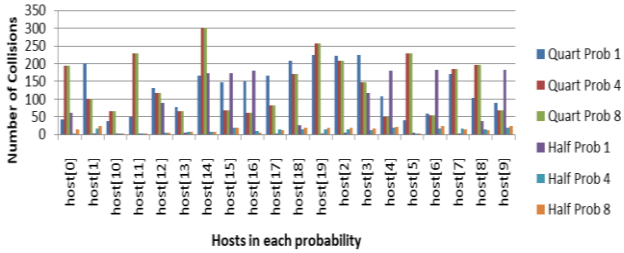

Fig. 7. Number of collisions in TCP network.

B. Results When Using TCP Protocol

In this part we will discuss TCP scenario. In Fig. 5, Fig. 6, and Fig. 7, we can illustrate: packet drop, average loss rate and number of collision.

It is only logical that the number of dropped packets rises in perfect agreement with the number of attackers in the network, as shown in Fig. 5, and with the change in the probability of losing the utilized packets 1, 4, and 8, we also see a convergence between the levels of all these possibilities.

For real-time intra-network communications flows, the PLR is an essential performance metric. Because the smoothness and simplicity of transmission of these data streams are assured, the number of lost or missing packets during transmission must be maintained to the minimum. During the transmission period, it is determined by the PLR computation as follows:

$$\text{PLR} = \frac{\text{Ntx}}{\text{Nrx}} \times 100\%$$

Ntx and Nrx denote the total number of packets transmitted and received, respectively. This analysis may be completed quickly by extracting all real-time packet sizes transmitted and received.

The packet collision rate is the number of data packet collisions that occur in a network during a particular time period. This will show how frequently data packets are collided or lost due to collisions. The packet collision rate is expressed as a percentage of data packets successfully delivered.

When two or more nodes in a network try to send data at the same time, packet collisions occur, resulting in collisions and possibly data loss. Nodes may have to resend packets as a result of this, which can have a detrimental influence on system performance.

Because the process is irregular inside the wireless network and is not restricted in time for transmitting and receiving, we observe that the collision counts are random in a TCP network, but we also note that the collisions are within the usual range in any network environment.

VIII. Conclusion

Maintaining the security of wireless network is a never-ending effort. In reality, no single effective security method exists. When a new technology is first launched, hackers examine it for weaknesses and then put together a bundle of software and scripts to try to attack those flaws. These technologies, which are disseminated through an open source network, are becoming more centralized, mechanized, and widely accessible over time. As a consequence, anyone may readily download it. Therefore, we will never be ready to overcome all threats and vulnerabilities, and even if we do, we will waste money defending against certain low-probability, low-impact cyberattacks. On the other hand, if we focus on the most critical problems first, attackers may shift their attention to less difficult targets. As a result, efficient WLAN security will always involve a delicate balance between allowable risks and risk-mitigation techniques in both business and home network. By better understanding company risks, taking action to avoid the most significant and frequent attacks, and implementing industry standards, we can enhance our security solutions. In this

study, an OMNET++ simulator was used to reproduce a based WLAN network with an IEEE 802.11 Wireless LAN working protocol for FTP and TCP applications. The study's main objective was to see how various network standards, such as data transmission delay, enhanced significantly, responsiveness, TCP abort, and throughput, fared in terms of latency. The results demonstrated that improving a wireless network's data throughput lowers time, media access latency, and queue size.

CONFLICT OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] A. Varga, "OMNeT++," in *Modeling and Tools for Network Simulation*, Springer, Berlin, Heidelberg, 2010, pp. 35-59.

[2] J. H. Yeh, J. C. Chen, and C. C. Lee, "WLAN standards," *IEEE Potentials*, vol. 22, no. 4, pp. 16-22, 2003.

[3] A. U. Syed, "Very high throughput (VHT) multi-user multiple input multiple output (MU-MIMO) communication in 802.11 ac," thesis, Simon Fraser University, Canada, 2015.

[4] Y. Xiao, "IEEE 802.11 n: Enhancements for higher throughput in wireless LANs," *IEEE Wireless Communications*, vol. 12, no. 6, pp. 82-91, 2005.

[5] F. T. Sheldon, J. M. Weber, S. M. Yoo, and W. D. Pan, "The insecurity of wireless networks," *IEEE Security and Privacy*, vol. 10, no. 4, pp. 54-61, 2012.

[6] P. Feng, "Wireless LAN security issues and solutions," in *Proc. IEEE Symposium on Robotics and Applications (ISRA)*, 2012, pp. 921-924.

[7] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546-556, 2014.

[8] L. Wang, B. Srinivasan, and N. Bhattacharjee, "Security analysis and improvements on WLANs," *Journal of Networks*, vol. 6, no. 3, pp. 470, 2011.

[9] M. Tigner, H. Wimmer, and C. M. Rebman, "Analysis of kali linux penetration tools: A survey of hacking tools," in *Proc. International Conference on Electrical, Computer and Energy Technologies*, 2021, pp. 1-6.

[10] D. S. Rao and V. B. Hency, "A novel QoE based cross-layer scheduling scheme for video applications in 802.11 wireless LANs," *SN Appl. Sci*, vol. 3, 2021.

[11] D. He, Z. Deng, Y. Zhang, S. Chan, Y. Cheng, and N. Guizani, "Smart contract vulnerability analysis and security audit," *IEEE Network*, vol. 34, no. 5, pp. 276-282, 2020.

[12] H. I. Bulbul, I. Batmaz, and M. Ozel, "Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols," presented at the 1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, And Multimedia and Workshop, January 2008.

[13] A. Agrawal, A. H. Seh, A. Baz, H. Alhakami, W. Alhakami, M. Baz, R. Kumar, and R. A. Khan, "Software security estimation using the hybrid fuzzy ANP-TOPSIS approach: Design tactics perspective," *Symmetry*, vol. 12, no. 4, p. 598, 2020.

[14] Y. Arafat, K. S. Yeaser, A. Rahman, and A. Dasgupta, "A machine learning based approach for protecting wireless networks against DoS attacks," in *Proc. 7th International Conference on Networking, Systems and Security*, New York, USA, 2020, pp. 126–132.

[15] T. Li, C. Xue, Y. Li, and O. A. Dobre, "Defending against randomly located eavesdroppers by establishing a protecting region," *Sensors*, vol. 20, no. 2, 2020.

[16] P. Arpaia, F. Bonavolontà, and A. Cioffi, "Advanced encryption standard problems in protecting internet of things sensor networks," *Measurement*, vol. 161, pp. 1-9, Sep. 2020.

[17] A. F. Rochim, B. Harijadi, Y. P. Purbanugraha, S. Fuad, and K. A. Nugroho, "Performance comparison of wireless protocol IEEE 802.11ax vs 802.11ac," in *Proc. International Conference on Smart Technology and Applications (ICoSTA)*, 2020.

[18] Y. B. Bai, A. Kealy, and L. Holden, "Evaluation and correction of smartphone-based fine time range measurements," *International Journal of Image and Data Fusion*, vol. 12, no. 3, pp. 185-202, Dec. 2020.

[19] P. Satam and S. Hariri, "WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol," *IEEE Trans. on Network and Service Management*, vol. 18, no. 1, pp. 1077-1091, March 2021.

[20] J. A. R. P. de Carvalho, H. Veiga, C. F. R. Pacheco, and A. D. Reis, "Extended performance research on IEEE 802.11 a WPA multi-node laboratory links," in *Transactions on Engineering Technologies*, S. I. Ao, L. Gelman, and H. K. Kim, Eds., Springer, Singapore, 2021, pp. 175-186.

[21] R. Nazir, K. Kumar, S. David, and M. Ali, "Survey on wireless network security," *Archives of Computational Methods in Engineering*, 2021.

[22] P. Feng, "Wireless LAN security issues and solutions," in *Proc. IEEE Symposium on Robotics and Applications (ISRA)*, 2012, pp. 921-924.

[23] A. Arora, "Preventing wireless deauthentication attacks over 802.11 networks," arXiv:1901.07301, 2008.

[24] M. K. Kissi and M. Asante, "Penetration testing of IEEE 802.11 encryption protocols using Kali Linux hacking tools," *International Journal of Computer Applications*, vol. 176, no. 32, pp. 26-33, 2020.

[25] B. Forouzan, *Data Communications & Networking*, 4th ed. New York: McGraw-Hill, 2008, ch. 30-31.

[26] H. Hou, Y. Xu, M. Chen, *et al*., "Hierarchical long short-term memory network for cyberattack detection," *IEEE Access*, vol. 8, pp. 90907-90913, Mar. 2020.

[27] N. M. Chayal and N. P. Patel, "Review of machine learning and data mining methods to predict different cyberattacks," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 52, pp. 43–51, June 2020.

[28] U. Saxena, J. Sodhi, and Y. Singh, "An analysis of DDoS attacks in a smart home networks," in *Proc. 10th International Conference on Cloud Computing, Data Science & Engineering*, 2020, pp. 272-276.

Iyas Alodat was born in 1983 in Irbid, Jordan. He started his career at the Jerash University in 2016. He is working as assistant professor in computer science and information technology, Jerash, Jordan after he received his Ph.D. degree in 2015 from Craiova University, Romania. He has published many papers in computer network, system modeling, performance evaluation and their applications in such biomedical areas also he is interested in electrical networks and computer systems.