ARTICLE

JOURNAL OF UNIVERSITY OF BABYLON

For ENGINEERING SCIENCES (JUBES)

Vol.30, No.4.| 2022

Wireless Networks (Attacks –Security): A Review

Zina A. Saleh[1], Bashar H. Hameed[2]

1 Department of Studies and Planning, Presidency of the University of Babylon, Iraq

Email: zina.badi@uobabylon.edu.iq

2 Department of Construction and Projects, Presidency of the University of Babylon, Iraq

Email*:* basharhadi@uobabylon.edu.iq

Received:	**20/10/2022**	**Accepted:**	**29/11/2022**	**Published:**	**2/12/2022**

Abstract

Wireless network security is an important, influential, and effective part of defending wireless networks from intrusions and security holes caused by hackers and attackers. This paper conducted a review of wireless network security requirements, including authentication, confidentiality, availability, and integrity, as well as attacks against wireless networks based on these requirements, most notably Man in the Middle Attack, Eavesdropping, and Denial of Service attack. In addition, some steps were reviewed that would protect and secure wireless networks from hacker attacks.

Keywords: Wireless threats, Network Security, Network Attack, and Security Requirements.

1. Introduction

The wireless connection allows the network user to enjoy a great deal of free movement as opposed to a wired connection. Now wireless technologies are dominant in the areas of wired networks. Today, wireless networks have many advantages over wired networks such as portability, cost and flexibility .Wireless networks allow users to access mobile data extremely easily without the usage of wires because data is stored centrally while the user is moving , as shown in Figure (1). As the number of users for networks is constantly increasing, message security has become the primary concern. Devices consisting of a wireless network are available to potential intruders for the purpose of unintentionally obtaining information [1] . Wireless security design is usually based on the encryption systems . As such, the use of shared secrets as a cryptographic foundation is the norm these days in wireless safety [2].

مـــجلة جـــامعة بـــابل للعلـــوم الهندسية مـــجلة جـــامعة بـــابل للعلـــوم الهندسية مـــجلة جـــامعة بـــابل للعلـــوم الهندسية

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

مجلـة جـامعة بـابـل للعلـــوم الهندسية مـجلـة جـامعة بـابـل للعلـــوم الهندسية مـجلـة جـامعة بـابـل للعلـــوم الهندسية

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

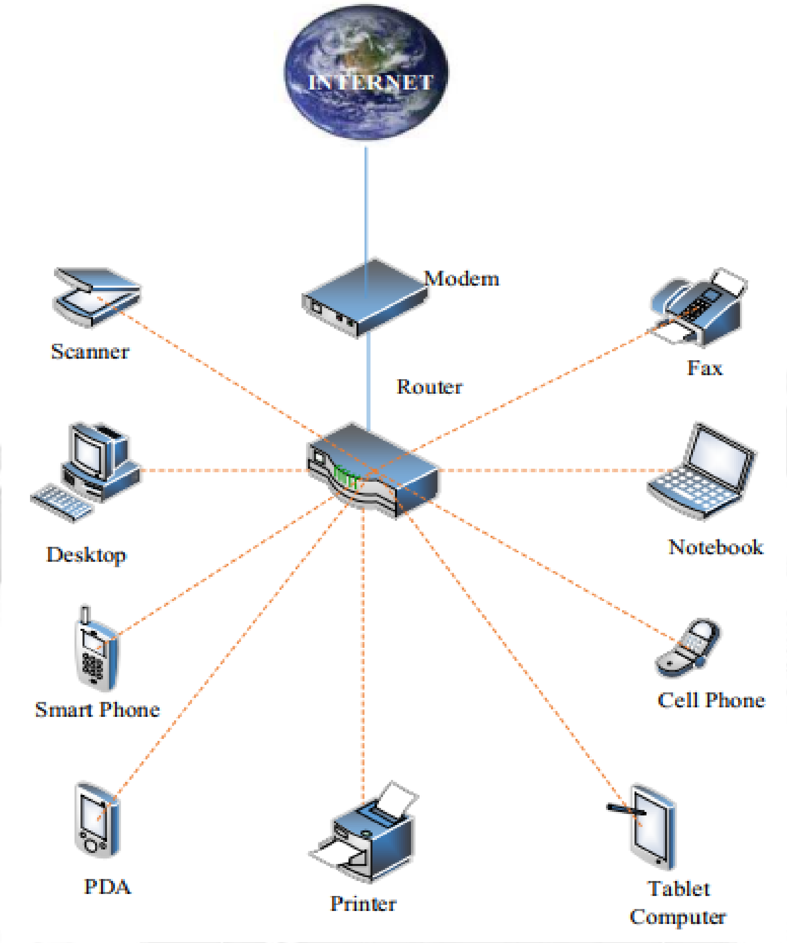

Figure (1) A Wireless Network [1]

Wireless networks can be configured and reconfigured more quickly, cheaply, and easily. Wireless technologies, however, also produce new threats and alter the information security risk profile. For example, the risk of eavesdropping is higher in wireless networks than it is in wired ones since communications occur "over the air" via radio frequencies. It could jeopardize confidentially if the communication is not encrypted or is just weakly encrypted because it can be easily read by an attacker [3].

As shown in Figure 2, a wireless network has four main parts: users, client devices (PDAs, laptops, etc.), access points that link to the organizational network, and radio frequency data transmission. Each of these elements may offer a potential attack route that could jeopardize any one of the four main objectives of confidentiality, authenticity, integrity, and availability [3].

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

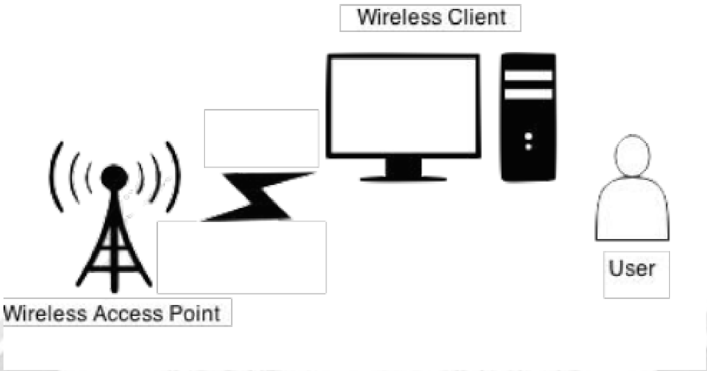

Figure (2) Wireless networking components [3]

This paper is arranged and organized in 5 sections. In Section 2 there is a mention of the security requirements in wireless networks and a brief explanation of each one of them. Section 3 deals with wireless network attacks with a simple explanation of each one. Section 4 talks about securing and protecting wireless networks in several points. Finally, in Section 5, some conclusions are presented.

2. Requirements for Wireless Network Security

Information is shared between authorized users in wireless networks, however because the wireless medium is broadcast, many malicious threats might compromise this process [4-5].

In general, secure wireless communications must satisfy the requirements for confidentiality , authenticity, availability , and integrity, [6], as shown below:

2.1 Authenticity

The property of being authentic and being able to be verified and trusted, confidence in the authenticity of a transmission, a message, or originator of the message. This means verifying that the message came from a trusted source or legitimate user [1] ,which refers to distinguishing between authorized users and unauthorized users by verifying the real identity of a network user [7].

2.2 Confidentiality

This term consists of two related concepts:

a) **Data confidentiality:** means that access to data is restricted only to the intended users, while preventing information from being disclosed to unauthorized entities and destinations [8]. where the original data, which is frequently referred to as plain text, is encrypted using an encryption algorithm and a secret key that is only shared with the intended recipient. Then, the ciphered plaintext (referred to as cipher text) to the destination which then decrypts the received cipher text with the secret key. The eavesdropper cannot decipher the plaintext from the cipher text heard since he is unaware of the secret key [9-10].

b) Privacy: Ensures that individuals have influence and control over what information about them can be collected and stored, and who can disclose that information and to whom [1-9].

2.3 Integrity:

The integrity of the transmitted data must be received by the receiver, such as the one sent by the sender, in an accurate, reliable manner without any change or modification in the data[11- 12].

2.4 Availability:

Availability denotes the fact that, upon request, authorized users can immediately connect to the wireless network from any location and at any time. It makes sure that systems operate quickly and that service is not withheld from authorized users. The network has to function constantly. [12-13].

3. Wireless Networks Attacks

3.1 Authenticity Attacks:

a) Application Login Theft

This attack can occur by hijacking the username and passwords of the user's email identifiers by using clear-text-application protocols [14].

b) Password Guessing

It is accomplished by repeatedly trying to guess the user's password using a captured identity by the attacker [15].

c) Encrypted-Authentication-Protocol (EAP) Downgrade

It includes using a fake EAP response to force a wireless server to display weaker authentication [16].

3.2 Availability Attacks:

a) Access-point Theft

It is a fundamental availability attack that involves physically eliminating an access-point from a local area. [17].

b) Denial-of Service (DOS)

This kind of attack works by exploiting the Carrier-Sense-Multiple-Access (CSMA) technicality into thinking a channel is busy. This can be done unintentionally or intentionally [18].

مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

There are accidental interferences as a result of wireless networks using the 2.4 GHz band, which is very common in all wireless and radio services. But, there is also intentional interference by some attackers in the form of a flood attack, as shown in Figure (3).

There are some other methods of Denial-of Service attacks[18]:

- **Beacon Flood:**

This technique involves the attacker producing a large number of fake wireless beacons to make it harder for the stations to locate the genuine access-point.

- **De-authenticate Flood:**

This attack method involves flooding the stations with fake de-authenticates or de-associates to separate the genuine user from an access-point.

- **EAP Start Flood:**

In this technique, the attacker consumes resources or destroys the target by flooding the access-point with EAP start messages.

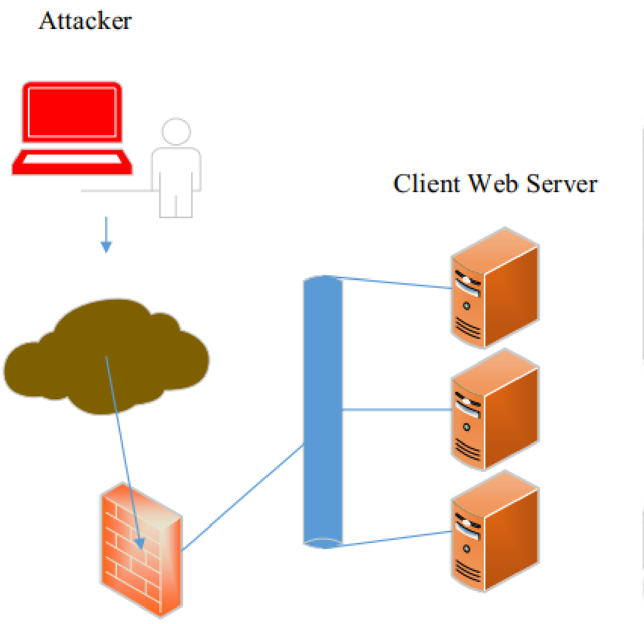

Figure (3) Denial of Service Attack [18]

3.3 Confidentiality Attack:

a) Eavesdropping

It is intercepting a private conversation in real time without authorization such as video meeting, as illustrated in Figure (4). (Voice Over Internet Protocol) systems are the principle goal of Eavesdropping attack because these systems are not encrypted. As a result, the attacker will find it very easy for him to intercept calls [19].

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

مجلة جامعة بابل للعلوم الهندسية

There are two types of eavesdropping techniques:

- **Passive Eavesdropping:** Where in this technique the eavesdropper monitors the communication without interfering with the communication channel. It is difficult to detect a passive eavesdropper, because its presence does not produce anything that can be observed [20].
- **Active Eavesdropping:** The ability to monitor the communication medium and alter its contents is provided by active eavesdropping techniques. For example, an active eavesdropper might have the ability to add messages, change the contents of an intercepted connection, or delete messages before they are received [20].

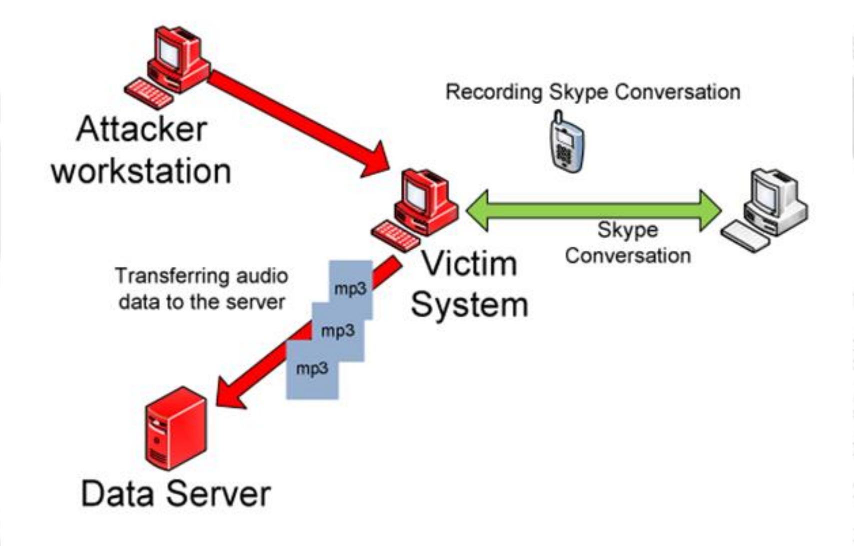

Figure (4) Eavesdropping [19]

b) Man -in the -Middle Attack (MITM)

In MITM attack, the attacker is positioned between two hosts to gain a connection. This attack is comparable to when two people throw a ball at each other and a third person tries to catch it between them, The attacker will attempt to access and modify the message before sending it back, as shown in the figure (5).

MITM can happen as jamming through continually sending signals to active wireless access points ,with supplying a clear signal from other counterfeit access-points. It will trick the server into thinking it is a client and the client into thinking it is a server and it will also tamper with the messages transmitted on both ends. [21].

ISSN: 2616 - 9916
www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

مجلة جامعة بابل للعلوم الهندسية
ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

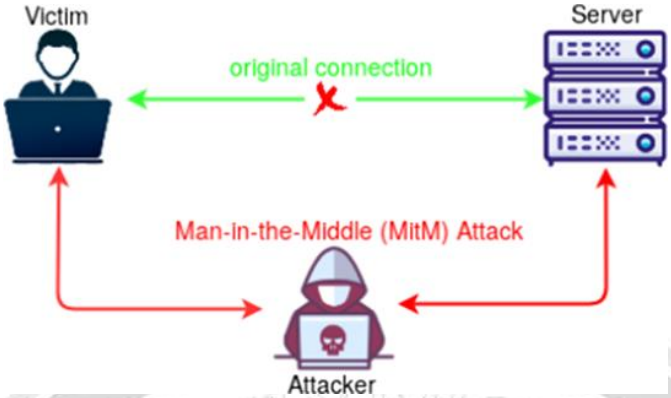

Figure (5) Man in the Middle Attack [21]

3.4 Integrity Attacks:

a) Re-Authentication

The Extensible Authentication Protocol (EAP) identity will be captured by the attacker as well as Remote Authentication Dial In User Service (RADIUS). After storing the authentication information, the attacker will monitor the traffic to obtain additional authentications [22] .

b) Replaying data

This attack involves the capture of data frames including sensitive and private information, which the attacker then modifies and saves for later use [23] .

c) Injection of Frames

In this kind of attack, the attacker crafts the original transmission while injecting their own frames between them so that forged frames can be spent. For illustration, when a person tries to access their bank's webpage, it can seem to them to be an authentic web page, but in reality, the attacker has injected their own frames, so what appears to be an original page is not. The attacker captures the user's login information when they attempt to enter it. [24] .

4. Securing Wireless Networks

With the tremendous development in wireless technology, the need for security of wireless networks has become more necessary and important than before because security protects the wireless network from all forms and different types of attacks and threats that are developing on a daily basis. Systems can be protected from a variety of potential dangers by security, which can stop illegal access to data and information. However, wireless networks get many security issues, From time to time, new security vulnerabilities will appear in the current wireless standards[25].

To protect and secure wireless networks, there are several aspects, including [1-3-25]:

1- Using encryption is one of the best methods to keep networks and systems safe from attackers and intruders. It encrypts all wireless traffic to safeguard the secrecy of information

مـجـلـة جـــامعة بــابـل للعلـــوم الهندسية مـجـلـة جـــامعة بــابـل للعلـــوم الهندسية مـجـلـة جـــامعة بــابـل للعلـــوم الهندسية

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

exchanged across wireless networks. In fact, most access points, wireless routers, and base stations have an integrated encryption mechanism.

Encryption is a critical component of wireless security techniques for network protection. security protocols help to achieve the security process in wireless networks. There are numerous security issues involved with today's wireless protocols and encryption technologies. Several protocols have been developed to accomplish the needed wireless security. These protocols contain security mechanisms in terms of authentication and encryption.

2- Use anti-virus, firewall and spyware programs while keeping them up-to-date, especially on computers.

3- An identifier broadcast feature included in the majority of wireless routers delivers signal information to any nearby device that declares its presence. In the event if the individual already utilizing the network is aware of its existence, there is no need to disseminate this information. ID broadcast needs to be disabled since it can be hijacked and used by attackers on wireless networks in homes.

4- Changing the router's (default password) which is pre-set by the manufacturer because hackers know the default passwords. Longer and more complicated passwords are preferable because they are harder for hackers to guess and crack.

5- Turn off the wireless network when not in use, as hackers and intruders cannot access the router when it is turned off. Thus, reducing the possibility of network penetration.

5. Conclusions

Wireless networks provide many opportunities to increase productivity as well cut costs. In this paper, the security requirements of wireless networks were reviewed, which are represented by authentication, confidentiality, availability, and integrity. Briefly mentioned aspects of wireless network attacks based on these requirements. It also reviewed in several points the most prominent ways to protect and secure wireless networks from security holes and intruders.

This review can help future scholars research, investigate, and strive for new and modern security techniques.

6. References

[1] S. Sharma, R. Mishra, and K. Singh, “A Review on Wireless Network Security”, 9th International Conference on Heterogeneous Networking for Quality, Reliability, Security, Robustness, pp. 668–681, 2013.

[2] G. Green, R. J. Fischer, “Introduction to Security, Fourth Edition”, NCJ, no. 104481,1987.

[3] M-K Choi, R.J. Robles, C.-H. Hong, T.-H. Kim, “Wireless Network Security:Vulnerabilities, Threats and Countermeasures”, International Journal of Multimedia and Ubiquitous Engineering Vol. 3, no. 3, pp. 77–85, July, 2008.

[4] D. Ma and, G. Tsudik, “Security and privacy in emerging wireless networks,” IEEE Wireless Communication, vol. 17, no. 5, pp. 12–21, 2010.

[5] H. Kumar, D. Sarma, A. Kar, “Security threats in wireless sensor networks,” EEE Aerospace and Electronic Systems Magazine, vol. 23, no. 6, pp. 39–45, Jun. 2008.

[6] Y.-S. Shiu ,S. Y. Chang, H.-C. Wu, S. C.-H. Huang, “Physical layer securityin wireless networks: A tutorial,” IEEE Wireless Communications, vol. 18, no. 2, pp.66–74, Apr. 2011.

[7] Y. Jiang, C. Lin, X. Shen, M. Shi, “Mutual authentication and key exchange protocols for roaming services in wireless networks,” IEEE Transactions on Wireless Communications, vol.5, no. 9, pp. 2569–2577, Sep. 2006.

[8] W. Stalling, “Cryptography and Network Security: Principles and Practices, 3rd”, Englewood Cliffs, NJ, USA: Prentice-Hall, Jan. 2010.

[9] D. Fang, Y. Qian, R.Q. Hu “ Security for 5G Mobile Wireless Networks,” IEEE Access, vol.6, pp. 4850–4874, 2017.

[10] D.V. Medhane, A.K. Sangaiah , “Source node position confidentiality aspects in wireless networks: an extended review”, International Journal of High Performance Systems Architecture, vol. 6, no. 2, pp. 61–81, Jan. 2016.

[11] D. Dzung, M. Naedele, T. Von Hoff, M. Crevatin, “Security for industrial communications systems” , Proceedings of the IEEE, vol. 93, no. 6, pp. 1152–1177, Jun. 2005.

[12] R. Nazir, A. A. laghari, K. Kumar, S. David, M. Ali, , “Survey on Wireless Network Security”, Archives of Computational Methods in Engineering, vol. 29, no. 3, pp. 1591–1610, May 2022.

[13] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” IEEE Computer,vol. 35, no. 10, pp. 54–62, Oct. 2002.

[14] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, “Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks ”, IEEE International Conference on Computational Intelligence and Computing Research, 2013.

[15] J.-L. Tsai, N.-W. Lo, T.-C. Wu, “A New Password-Based Multi-server Authentication Scheme Robust to Password Guessing Attacks ”, Wireless Personal Communications, vol. 71, pp. 1977–1988, 2013.

[16] F. A. Perez,“Security in current commercial wireless networks: A survey. ”, School of Electrical and Computer Engineering, Purdue University West Lafayette, pp. 1–62, 2004.

[17] A. Gupta, R. Kumar, P. Gandotra, S. Jain, “Bandwidth Spoofing and Intrusion Detection System for Multi Stage 5G Wireless Communication Network”, IEEE Transactions on Vehicular Technology, vol. 67, no. 1, 2017.

[18] J. Luo, X. Yang, “The New Shrew attack: A new type of low-rate TCP-Targeted DoS attack”, IEEE International Conference on Communications (ICC), 2014.

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

مـجلـة جـامعة بـابل للعلـــوم الهندسية مـجلـة جـامعة بـابل للعلـــوم الهندسية مـجلـة جـامعة بـابل للعلـــوم الهندسية

[19] S. Ohno, Y. Wakasa, S. Q. Yan, E. Manasseh, "Optimization of transmit signals to interfere eavesdropping in a wireless LAN " IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2014.

[20] M. Sherr, "Eavesdropping" ,Encyclopedia of Cryptography and Security, pp 378–379, 2011.

[21] F. Tommasi, C. Catalano, I. Taurino, "Browser-in-the-Middle (BitM) attack", International Journal of Information Security, vol. 21, no. 2, pp 179–189, 2022.

[22] S. Chandrasekaran, K.I. Ramachandran, S. Adarsh, A. K. Puranik, "Avoidance of Replay attack in CAN protocol using Authenticated Encryption", 11th International Conference on Computing and Networking Technology (ICCNT), 2020.

[23] H. Guo, Z.-H. Pang, J. Sun, J. Li, "An Output-Coding-Based Detection Scheme Against Replay Attacks in Cyber-Physical Systems", IEEE Transactions on Circuits and Systems, vol.68, no. 10, 2021.

[24] Rashmi, N. Bajpai, "A Keyword Driven Framework for Testing Web Applications", International Journal of Advanced Computer Science and Applications (IJACSA), vol. 3, no.3, pp. 8-14 , 2012.

[25] U. Kumar, S. Gambhir, "A Literature Review of Security Threats to Wireless Networks", International Journal of Future Generation Communication and Networking, vol.7, no.4, pp.25-34, 2014.

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية مجلة جامعة بابل للعلوم الهندسية

ISSN: 2616 - 9916 | www.journalofbabylon.com | Journal.eng@uobabylon.edu.iq | info@journalofbabylon.com

الشبكات اللاسلكية (هجمات– أمن): بحث مراجعة

زينة عبد الحسين صالح

قسم الدراسات والتخطيط، رئاسة جامعة بابل، بابل، العراق

Email: zina.badi@uobabylon.edu.iq

بشار هادي حميد

قسم الاعمار والمشاريع، رئاسة جامعة بابل، بابل ، العراق

Email: basharhadi@uobabylon.edu.iq

الخلاصة

يعد أمن الشبكات اللاسلكية جزءًا مهمًا ومؤثرًا وفعالًا في حماية الشبكات اللاسلكية من عمليات التطفل والثغرات الأمنية التي يسببها المتسللون والمهاجمون. أجرى هذا البحث مراجعة لمتطلبات أمان الشبكة اللاسلكية، بما في ذلك المصادقة والسرية والتوافر والنزاهة، بالإضافة إلى الهجمات ضد الشبكات اللاسلكية بناءً على هذه المتطلبات، وأبرزها هجوم الرجل في الوسط، والتنصت، وهجوم رفض الخدمة. بالإضافة إلى ذلك، تمت مراجعة بعض الخطوات التي من شأنها حماية وتأمين الشبكات اللاسلكية من هجمات المتطفلين.

الكلمات الدالة: التهديدات اللاسلكية، أمن الشبكات، هجوم الشبكات، متطلبات الأمن.