Types of Attacks in Wireless Communication Networks

Teeb Hussein Hadi
IT Department, Middle Technical University, Technical College of Management, Baghdad, Iraq.
E-mail: eng.teebhussien@mtu.edu.iq

Received August 16, 2021; Accepted November 30, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19051

Abstract

One of the most important types that used to transfer data between nodes without using wires is a “wireless communication network”, where the transmission of data is censored remotely by using electromagnetic waves such as radio waves that usually implemented in the physical layer of the network. Continuous improvements in wireless network technology have reduced the security and speed differences between types of networks (wired and wireless), but in turn, increased security threats to wirelessly transmitted data. Wireless networks are weak in terms of "privacy protection" because anyone who is within the coverage area of a wireless network can attempt to break into that network. Hacking incidents have been reported frequently in places with shared free networks, and it has been observed that the places of open distributed networks of the Internet are most at risk of complete penetration of your phone or PC data. To solve this problem, several programs have been developed that provide protection for wireless networks that differ in terms of security. Some of them did not provide sufficient protection for wireless networks, such as Wired Equivalent Privacy (WEP), and others made progress in preventing intrusions compared to their predecessors, such as Wi-Fi Protected Access (WPA).

Keywords

Passive Attacks, Active Attacks, Wireless Networks, Information Security.

Introduction

To date, wireless communication networks have received great development in the field of data transmission. This is due to the convenience of their use, low cost and acceptable bandwidth. Based on the current dynamics of development, you can conclude that the number and prevalence of wireless networks will soon time will surpass wired networks. Development of wireless networks and systems based on them (Kaisa et al., 2019).

Wireless computer networks are a technology that allows you to create computer networks that fully comply with the standards for conventional wired networks, without the need for cabling. Wireless Networks characterized by wireless links, mobility of nodes and dynamic network topologies (Mumtaz & Teeb, 2014). Wireless technology allows data to be transmitted over the air, rather than over wires. It is a technique that allows individuals, telecommunications networks and businesses to limit the use of cables between various locations (Liang et al., 2008).

Wireless networks provide data exchange between local computer networks when the use of traditional cable technologies is difficult or impractical (expensive). An example of effective use of wireless radio access technology is to provide communication between segments of local networks with a lack of funds, lack of permission to carry out cable works or the refusal of the telephone exchange to lease a dedicated channel (Zhang et al., 2019). Indoors cable laying may not be possible due to non-separable floor or if prohibited installation work. The use of the appropriate solution method depends on the characteristics of the connection (transmission speed, maximum throughput, cost of infrastructure and connected equipment, security, flexibility of installation and use, electricity consumption and autonomy, etc.) (Teeb, 2017).

Any wireless network is based on its protocol. As a rule, the protocol regulates the network topology, routing, addressing, the format of transmitted packetsو Arranging network nodes for quick access to the data transmission channel, a set of control commands for network nodes and information security system (Alimul et al., 2014).

These dynamics directly affect information security requirements in wireless networks. In this paper, the wireless communication definition, their types, equipment, security attacks in wireless networks are considered.

Wireless Networks Concepts

As well as networks based on the use of wires or optical fibers, wireless networks transmit information between computer devices. This information can be in any form like e-mail, video, or voice messages, etc. In most cases, wireless networks transmit data, such as e-mails and files, but as wireless network performance improves, they are capable of transmitting video signals as well as providing telephone communications (Pathan et al., 2006).

Wireless networks can be implemented by remote control with information transmission systems using electromagnetic radio waves or infrared (IR) range as the carrier of this information signal, implementing it in the physical layer of the network. Moreover, the actual transmission medium (air) is transparent to the user. Now many manufacturers integrate network interface cards (NIC), so-called network adapters, and antennas into computer devices in such a way that they are not visible to the user. It makes wireless devices mobile and easy to use (Yang et al., 2006).

Depending on the size of the physical zone in which they are capable of communication provide, wireless networks fall into several categories (Jordi, 2009):

- "Wireless Personal Area Network" (PAN).
- "Wireless Local Area Network" (LAN).
- "Wireless Metropolitan Area Network" (MAN).
- "Wireless Wide Area Network" (WAN).

These terms are just extensions of generalized forms of wired networks (LAN and WAN) that were used long before the advent of wireless networks as shown in fig.1.

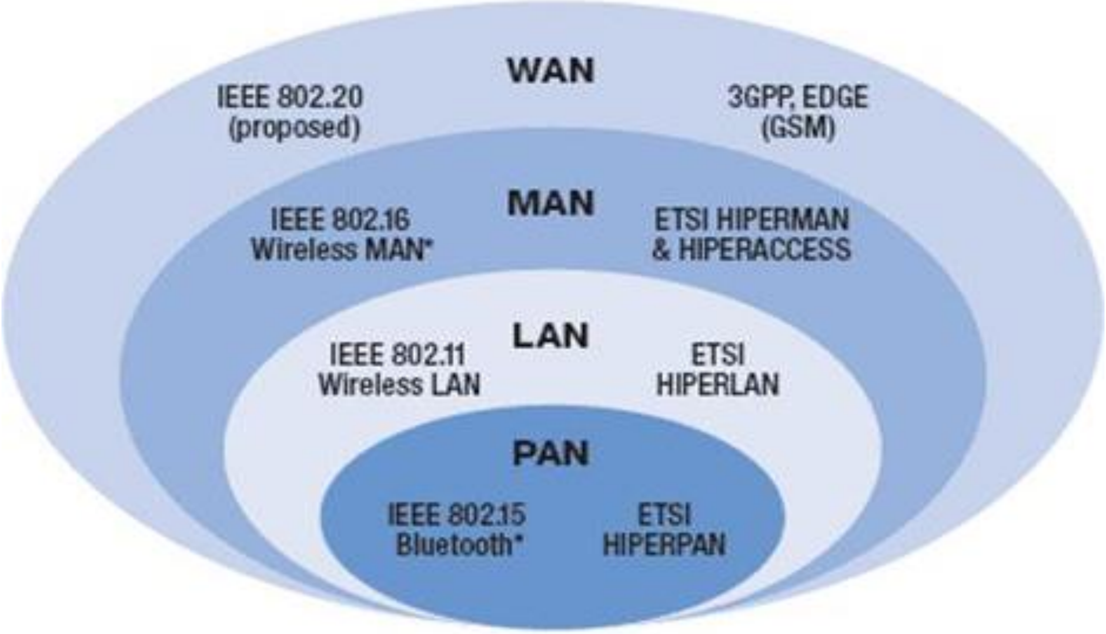

Fig. 1 Wireless Networks Classification

Table 1 gives a brief description of the varieties of such networks. Each type wireless network has features that complement other networks, due to which various network requirements are met.

Cat.	Max range	Flow rate	Uses	Standards	connectivity
WPAN	a few tens of m	1 Mbit / s	Particular network	IEEE 802.15 (Bluetooth), NFC, ETSI HyperPan	Bluetooth, ZigBee and Infrared
WLAN	500 m	over 50 Mbit / s	Internal networks, specific to a building (either as corporate network, either as home network)	IEEE 802.11 (a, b, c, ...) ETSI HyperLan	Cellular
WMAN	4 to 10 kilometers	from 1 to 10 Mbit / s	City, Campus, ... Interconnect several WLAN	IEEE 802.16 WiMax ETSI HyperMan	IEEE 802.16 WiMax
WWAN	Several hundreds of kms	from 1 to 10 Mbit / s	Regional, National Interconnects several cities	Based on technologies cellular	LTE

Equipment for Wireless Networks

In connection with the progressive development of wireless networks, more and more executives of companies, both small and large corporations, are faced with the task of introducing a wireless network or a full transition from cable infrastructure to a Wi-Fi network (Laura et al., 2009).

The main issue is the selection of equipment. Indeed, the reliability, performance and functionality of the network as a whole depends on the correct choice of system components. It is also worth considering the future when choosing equipment (Benyuan et al., 2010). Since the technology of electronic devices is developing faster and faster, it is necessary to lay in the project equipment models that can ensure the effective use of information technology not only now, but also in the near future. This will allow avoiding additional costs associated with network modernization in the future (Gerald et al., 2018).

Wireless devices can be controlled in one of the following ways:

- **A wireless button or switch.**
- **Wireless Assistant software.**
- **Operating system controls.**

Using the wireless button: Computer has at least one wireless device and one or two wireless indicators (depending on model). By default all built-in wireless devices are on, so when a computer is turning on, the wireless indicator will glow blue. The wireless light indicates the general status of the wireless devices, and not the state of an individual device. If the wireless light is blue light, it means that at least one wireless device is turned on. If the wireless light is off, and all wireless devices are off. By default, all built-in wireless devices are turned on, so the wireless connectivity allows all devices to be turned on and off at the same time wireless communication (Steve, 2007).

Using the Wireless Assistant software (only in some models): You can control the wireless devices by (WSA - Wireless Assistant software). To view the status of the wireless device, click the Wireless icon Assistant in Windows® Mobile Center.

Using operating room controls systems: Some operating systems provide a way to control embedded wireless devices and wireless connections (Bhagyavati et al., 2004).

Categories of Attack

If you know how to attack the enemy, you will be able to protect yourself. Information security has three dimensions, or three objectives that information security primarily serves and always works to achieve (confidentiality, safety, availability). When the hacker tries to attack the system, in any case, he tries to threaten one of these targets (Sreedhar et al., 2010). All types of attacks revolve around these targets because by losing one of them, the information security triangle is not available, and therefore the types of attacks can be divided according to the target that threatens it. So knowing the types of attacks can help you classify the type of threat. We will mention the most important types of threats to information security, which include (Aventail, 2004):

Snooping: Someone sent an e-mail to another person, and before it arrived, the hacker was able to attack the message and see it. Here we call this type of attack espionage. Espionage means the hacker's access to or interception of the transmitted information.

Traffic Analysis: Someone sent an email to another person, but it is encrypted, the hacker will not be able to understand it, but by following the data sent and analyzing it, the hacker was able to know the IP address of the sender and recipient. The IP address is not one of the data that is encrypted, but the message is only encrypted. In this case, we say that the hacker carried out an attack by analyzing the sent data because he tried to extract information from the sent data (Naseer, 2009).

Modification: Someone sent an email to another person asking them to transfer a sum of money to a specific address, the hacker managed to attack the message before it arrived and modify the address mentioned by the sender to another address belonging to the hacker, the hacker carried out the modification attack since he modified the sent data to serve his own interest.

Spoofing: Someone received an email addressing that it was from someone else they knew, but in fact it was sent by the hacker, here the hacker tried to disguise the identity of the sender in order to deceive the recipient. The hacker tried to attack the recipient by masquerading, and the masquerade may be in both directions, and I mean the sending and receiving directions. The hacker may disguise himself as the well-known person.

Repudiation: Someone sent someone to another person asking him to send a sum of money to a person known to him to give her the amount when they met, but when they met the known person denied that he was the one who sent this message! Here the well-known person turns into a hacker and is considered to have carried out a denial attack on the sending person as long as there is no way to prevent this denial. If you notice this attack has only two parties and there is no hacker between them (Zou et al., 2016).

Denial of Service: Threatening attacks on information security This type of attack is perhaps one of the most famous types of attacks, where the attacker tries to block the service by downloading it as much as it cannot bear. Five times that number per minute, and therefore the message-receiving service can't work or may slow it down.

Hacker attacks are also divided in another way into two types, based on the damage the attack will cause, If the attack will cause damage or modification to the message or the system, it is called an active attack, but if the goal of the attack is to obtain data only without causing any modification or damage, it is called a passive attack (Isaac et al., 2020).

Active attacks include: (Modification, Snooping, Replaying, Repudiation, Denial of Service), where passive attacks include: (Traffic Analysis and Snooping).

Active Attacks: In this type of attack, the attacker intercepts the connection and modifies the information to the point of damaging the systems, which poses a clear threat to the security of the system. Because of the large weaknesses, this attack is a difficult and harmful attack on the system and its resources, but one of its advantages shows a notification to the victim of the type of attack and the threat to Integrity and availability (Alferidah & Jhanjhi, 2020).

An active attack usually requires more effort and generally has a more difficult effect. An active attack is what is generally thought of when referring to "hacking". The attacker attempts to change or control the data and/or devices on which they reside. This is in contrast to a passive attack, where a hacker may listen in on communications or monitor other aspects of the network or its devices. Such as Denial of Service (DoS), distributed denial of service (DDoS), and Trojan horses (Furrakh et al., 2016).

Passive attacks: The function of this attack is to read or use information from the system, but it does not affect system resources and there is no modification to the content of messages and information because the threat of confidentiality and does not cause any harm to the system. You only need to monitor the transmission, you only need to monitor the transmission or collection of information. The eavesdropper does not make any changes to the data or the system as the attacker indulges in unauthorized eavesdropping (Kong et al., 2003).

Unlike an active attack, a passive attack is more difficult to detect because it does not involve any change in data or system resources. Thus, the attacking entity does not obtain any information about the attack. Although it can be prevented using encryption methods in which the data is first encrypted in an unintelligible language at the sender's end, and at the receiver's end, converted back into an intelligible language (Shafiullah et al., 2008).

The most common security risks and threats, you are generally more vulnerable to:

- Endpoint attacks: This type of attack uses Wi-Fi endpoints where attackers rely on the same hotspot that users share such as a tablet or phone, which are what attackers focus on in hacking wireless networks as any hacker can access your device through this same connection.
- Packet Sniffers Attacks: They are unfamiliar programs whose task is to monitor the strength of the network connection and the traffic of data and information within the network. These attacks are usually called packet analyzers. However, these programs are also a great hacking point for hackers to steal users' information like usernames and passwords through a method known as side jacking.
- Rogue WiFi Attacks: In this type of attack, the hackers set up a malicious wireless network with a specific goal, which is to steal users' data for the network. Usually,

this network uses attractive and attractive names that draw the attention of users and tempt them to connect to this network (Choi et al., 2008).

- Evil Twin Attacks: This type of attack is one of the strongest risks that threaten Wi-Fi network, where the attacker is making a fake network similar to the same real reliable network settings and the same as the work of Rogue Wifi but the latter uses attractive and distinctive names to attract users. Therefore when the user is connected to the network (feck network). Hackers will access your access or receive your network such as credit card details, bank information and passwords for applications and all other sensitive information.
- Man-in-the-middle Attacks: This type of species is attacked on Wi-Fi network, where hackers infiltrate among network users without knowing them as well as manipulating their common special statements, which are exchanged including confidentiality, but the right there is a third party spying on this special data (Gerald et al., 2018).

Unauthorized Access to Wireless Networks

There are several ways to gain unauthorized access to wireless networks, as well as recommendations for protecting against them.

First, we list the protection options that can be used on the access point to protect the network from foreign users:

- Device Dis-Announce - Don't let your wireless device announce its presence. Turn off SSID Broadcasting (Service Set Identifier), to prevent your wireless device from being publicly available (Akhil & Rakesh, 2015).
- SSID Cloaking - hide the network name. Only clients who know this name are allowed access.
- MAC Filtering - filtering by MAC addresses. Access is allowed only to clients whose network adapter addresses are recorded in the access point.
- Shared key Authentication - Shared key authentication. Access is only allowed to those clients who have been verified using the shared key (Martin, 2010).

It is important to note that these methods do not ensure the confidentiality of data transmitted over the network, they simply restrict access to the network (Lashkari et al., 2009). That is, even if all these tools are enabled on the access point, an attacker will be able, by turning on his wireless adapter in "monitor mode", to listen to the broadcast and catch all transmitted information. The following methods cryptographically protect data:

- WEP Is one of the most common ways to protect wireless networks, where encrypts all the detailed data through the network. It is his advantages that he uses a special key to encryption if the attacker is not known, you will not be able to decode, but at the same time from its negative that the encryption algorithm is very weak, as the key is breached by the striker in less than 5 minutes (Pavithran, 2015).
- WPA and WPA2 Pre-Shared Key A strong and formal enclave algorithm in the data encryption process to be used as a complex level in choosing the shared encryption key between the Internet users.
- WPA and WPA2 Enterprise are a variant of the previous system, but an external 802.1x EAP authenticator is used for identity verification, which allows the use of certificates, smart cards, etc. (Arash et al., 2009).

Conclusion

The ability of hackers to monitor traffic, gain unauthorized access to resources, and cause denial of service to wireless users are the challenges that need to be addressed. By using effective authentication and encryption mechanisms, you can significantly reduce the risk. This paper displayed the general concepts of a wireless network, the classification of wireless networks, and the general characteristics of the main types of hardware with main types of attack. However, it should be borne in mind that the required level of security depends on requirements for the network. The level of protection acceptable for a home network is completely inadequate to meet the security requirements of an enterprise network.

References

Lashkari, A.H., Mansoor, M., & Danesh, A. (2009). Wired equivalent privacy (WEP) versus Wi-Fi protected access (WPA). *In International Conference on Signal Processing Systems*, 445-449.

Gupta, A., & Jha, R.K. (2015). Security threats of wireless networks: A survey. *In International Conference on Computing, Communication & Automation*, 389-395.

limul Haque, A., Sinha, A.K., Singh, K.M., & Singh, N.K. (2014). Security Issues of Wireless Communication Networks. *International Journal of Electronics Communication and Computer Engineering, 5*(5), 1191-1196.

Lashkari, A.H., Danesh, M.M.S., & Samadi, B. (2009). A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i). *In 2nd IEEE international conference on computer science and information technology,* 48-52. http://doi.org/10.1109/ICCSIT.2009.5234856

Aventail (2004). *Practical solutions for securing your wireless network.* Aventail Technical White Paper.

Liu, B., Bestavros, A., Wang, J., & Du, D.Z. (2010). Wireless network algorithms, systems, and applications. *EURASIP Journal on Wireless Communications and Networking.* http://doi.org/10.1155/2010/589389

Summers, W.C., & DeJoie, A. (2004). Wireless security techniques: an overview. *In Proceedings of the 1st annual conference on Information security curriculum development*, 82-87.

Liang, C.J.M., Musăloiu-e, R., & Terzis, A. (2008). Typhoon: A reliable data dissemination protocol for wireless sensor networks. *In European Conference on Wireless Sensor Networks*, 268-285.

Alferidah, D.K., & Jhanjhi, N.Z. (2020). A Review on Security and Privacy Issues and Challenges in Internet of Things. *International Journal of Computer Science and Network Security IJCSNS, 20*(4), 263-286.

Shahzad, F., Pasha, M., & Ahmad, A. (2016). A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. *International Journal of Computer Science and Information Security (IJCSIS),* 14(12), 54-65.

Ijemaru, G.K., Adeyanju, I.A., Olusuyi, K.O., Ofusori, T.J., Ngharamike, E.T., & Sobowale, A.A. (2018). Security Challenges of Wireless Communications Networks: A Survey. *International Journal of Applied Engineering Research, 13*(8), 5680-5692.

Eian, I.C., Lim, K.Y., Yeap, M.X.L., Yeo, H.Q., & Fatima, Z. (2020). Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges. http://doi.org/10.20944/preprints202010.0018.v1

Kong, J., Hong, X., & Gerla, M. (2003). A new set of passive routing attacks in mobile ad hoc networks. *In IEEE Military Communications Conference. MILCOM 2003. 2,* 796-801.

Jordi, S. (2017). *Wireless networks*. Czech Technical University of Prague, Faculty of electrical engineering, 1st Edition, 2017, ISBN 978-80-01-06197-8.

Zhang, K., Chuai, G., Gao, W., Liu, X., Maimaiti, S., & Si, Z. (2019). A new method for traffic forecasting in urban wireless communication network. *EURASIP Journal on Wireless Communications and Networking, 2019*(1), 1-12.

Laura, C., Xavier M., Erik, G., & Alejandro R. (2009). *Cooperative Communications in Wireless Networks*", Hindawi Publishing Corporation. *EURASIP Journal on Wireless Communications and Networking,* http://doi.org/10.1155/2009/768314

Eian, M. (2010). A practical cryptographic denial of service attack against 802.11 i TKIP and CCMP. *In International Conference on Cryptology and Network Security*, 62-75.

Choi, M.K., Robles, R.J., Hong, C.H., & Kim, T.H. (2008). Wireless network security: Vulnerabilities, threats and countermeasures. *International Journal of Multimedia and Ubiquitous Engineering, 3*(3), 77-86.

Al-Mukhtar, M.M.A., & Hadi, T.H. (2014). A monitoring system using wireless sensor network. *Al-Nahrain Journal of Science, 17*(2), 219-226.

Pavithran, M. (2015). Advanced Attack Against Wireless Networks Wep, Wpa/Wpa2-Personal And Wpa/Wpa2-Enterprise. *International journal of scientific & technology research, 4*(8), 147-152.

Ahmad, N. (2009). *Security Issues in Wireless Systems*. Master's Thesis MEE09:47 in Electrical Engineering with emphasis on Telecommunications, Blekinge Institute of Technology of Computer Science & Information Technology.

Pathan, A.S.K., Lee, H.W., & Hong, C.S. (2006). Security in wireless sensor networks: issues and challenges. *In 8th International Conference Advanced Communication Technology, 2,* 1043-1048.

Liang, C., Zhang, Q., Ma, J., & Li, K. (2019). Research on neural network chaotic encryption algorithm in wireless network security communication. *EURASIP Journal on Wireless Communications and Networking, 2019*(1), 1-10.

Khan, S., Mast, N., Loo, K.K., & Silahuddin, A. (2008). Passive security threats and consequences in IEEE 802.11 wireless mesh networks. *Journal of Digital Content Technology and its Applications, 2*(3), 4-8.

Sreedhar, C., Verma, S.M., & Kasiviswanath, N. (2010). Potential security attacks on wireless networks and their countermeasure. *AIRCC's International Journal of Computer Science and Information Technology*, *2*(5), 76-89.

Rackley, S. (2007). *Wireless networking technology: From principles to successful implementation.* Newnes is an imprint of Elsevier Linacre House, Jordan Hill, Oxford. ISBN 13: 978-0-7506-6788-3.

Hadi, T.H. (2017). Manet and WSN: What makes them Different? *International Journal of Computer Networks and Wireless Communications (IJCNWC), 7*(6), 23-26.

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE, 104*(9), 1727-1765.

Xiao, Y., Lin, Y.B., & Du, D.Z. (2006). Wireless Network Security. *EURASIP Journal on Wireless Communications and Networking.* http://doi.org/10.1155/WCN/2006/48374