UDC 004.056

https://doi.org/10.33271/nvngu/2021-2/163

R. Yu. Korolkov,
orcid.org/0000-0001-5501-4600,
S. V. Kutsak,
orcid.org/0000-0001-5238-8957

National University "Zaporizhzhia Polytechnic", Zaporizhzhia, Ukraine, e-mail: romankor@zntu.edu.ua

ANALYSIS OF ATTACKS IN IEEE 802.11 NETWORKS AT DIFFERENT LEVELS OF OSI MODEL

Purpose. Analysis of the main types of vulnerabilities and definition of weaknesses in 802.11 wireless network security, identification of the causes of information loss or network failure as a result of attacks.

Methodology. Research on attacks at different levels of the OSI network model.

Findings. The main threats and attacks that are implemented at each level of the OSI network model, from the physical to the application level, are identified. 15 different attacks with a detailed description of the consequences of their implementation are considered. The correspondence between the levels of the OSI network model and peculiarities of the implementation of attacks is established.

Originality. The principle of increasing the abstraction level was used to systematize attacks on WLAN. First, the known attacks are compared according to the levels of the OSI network model and the destructive consequences of their implementation are indicated; secondly, four types of attacks (reconnaissance, availability, spoofing, man-in-the-middle) are identified, and thirdly, attacks are divided into categories of passive and active ones. This approach makes it possible to get a more conceptual understanding of security issues in wireless networks.

Practical value. The results obtained can be used to develop effective multi-level systems for detecting and preventing intrusions into WLAN.

Keywords: *attack, wireless network, network layer, spoofing, access point*

Introduction. The widespread use of mobile devices has led to an increase in Internet connections and the deployment of new computer networks and modernization of existing ones with a focus on wireless local area networks (WLAN). However, WLANs, unlike wired networks, are more vulnerable and have a number of threats that are inherent in this method of data transmission. Many wireless devices are used for illegal cybercrime, including malicious attacks, computer hacking, data forgery, theft of financial information, and others. Accordingly, as attackers develop and implement new attacks, there is a need to study them to further improve methods of protection against unauthorized actions in wireless networks. Therefore, the analysis of attacks on wireless networks, which includes classification and experimental research, is a topical problem.

Literature review. Quite a lot of publications are devoted to the study on individual threats and attacks on the WLAN, but there are not many works in which attempts are made to systematize existing attacks on the WLAN. In [1] the authors presented an overview of Denial of Service (DoS) attacks related to the IEEE 802.11i security standard. In [2], the authors analyze possible attacks aimed at the MAC layer. In [3, 4], the authors considered active and passive attacks on wireless networks. Work [5] discusses various security issues and vulnerabilities related with the IEEE 802.11 wireless LAN encryption standard, as well as common threats and attacks related to home and corporate wireless LAN systems. A detailed review of attacks and analysis of existing protocols and security algorithms for wireless networking standards such as Bluetooth, Wi-Fi, Wi-MAX and Long-Term Evolution (LTE) systems are provided by Yulong Zou, et al. in [6].

The purpose of our study is to review the main types of vulnerabilities and definition of weaknesses in the 802.11 wireless networks security, to analyse attacks at different levels of the OSI network model and systematize them, and indicate the destructive consequences of their implementation.

Analysis of network attacks. Unlike wired networks in which communication nodes are physically connected via cables, wireless networks use radio broadcasting and because of this are extremely vulnerable. Nevertheless, they have some similarities – they both use a multilevel architecture of interaction protocol of open systems OSI [7]. As a result, wired and wireless networks have some common security vulnerabilities due to their identical levels application, presentation, session, transport, and network. However, because the physical (PHY) level and data link (MAC) level of these networks are different, the vulnerabilities and attacks implemented at these levels will also differ, Fig. 1.

Different network protocols have different security vulnerabilities that correspond to the levels of the OSI model on which they operate [8].

To systematize possible attacks on wireless networks in our opinion, it is advisable to consider the attacks that are most often used at certain levels of the OSI model and classify them by type. This approach will allow obtaining results with which it is possible to improve the efficiency of Intrusion Detection Systems (IDS) and attack detection methods.

In wireless networks, a physical layer attack mainly involves a jamming attack [9]. At the MAC level and above, more sophisticated protocols-targeted attacks are possible. We have identified the 15 most important attacks in wireless networks, divided them into 2 categories – passive attacks and active attacks, and grouped them into 4 types, as shown in Fig. 2.

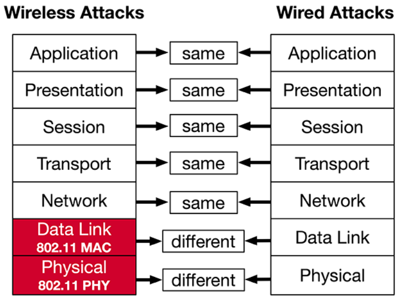


Fig. 1. OSI network model levels in terms of attacks in wireless and wired networks

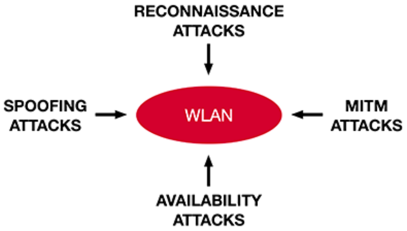


Fig. 2. Types of WLAN attacks

Passive attacks. Passive network attacks do not initialize data exchange with the nodes of the attacked network, do not interact with network data and do not change them [10]. Typically, attackers use passive attack methods to gather information and reconnaissance operations before carrying out the next attack – an active one.

Reconnaissance attacks. As soon as an attacker gains access to the transmission medium, a reconnaissance campaign begins. At this stage, the attacker usually spends time studying, i. e. identifying interesting computers – targets, collecting important IP addresses, MAC addresses and gaining insight into network resources and vulnerabilities. Reconnaissance actions allow the attacker to use the obtained information in the future.

Eavesdropping Attack. The physical layer is the lowest layer in the OSI architecture, which is used to determine the physical characteristics of signal transmission [6]. However, the broadcast nature of wireless communication makes the physical layer extremely vulnerable to eavesdropping attacks. During an eavesdropping attack, an attacker aims to intercept data transmission between legitimate users. In a WLAN, a communication session can be overheard when an attacker is within range of the network.

Cryptographic methods based on secret keys are commonly used to support confidential transmission. In particular, the source node and the destination node share a secret key, and the so-called plain text is first encrypted in the source node, which is then transmitted to the destination node. In this case, even if an attacker eavesdrops on the transmission of encrypted text, it remains difficult to extract plain text from the encrypted text without a secret key.

Password Attacks. These attacks are attempts to obtain a secret key to later connect to a wireless network, using its resources and carry out other attacks on internal network nodes. To obtain a secret key, an attacker must monitor certain data packets, and then continue the process of hacking keys offline.

Using a weak and unreliable password on Wi-Fi networks can be a serious problem, attracting the attention of attackers. In [11] the authors, on the example of hacking WPA2-PSK, show how weak passwords are subject to dictionary attacks and rude attacks.

Port Scanning. The port scan attack takes place within the network. As a result of the scan, the attacker finds all open ports, which can then be used to attack the target device.

Open ports can be used to deliver dangerous data and malware. We scanned the access point (AP) ports using the NMAP tool in Kali Linux, which is widely used to scan networks for vulnerabilities.

Command to launch this attack

nmap[*Scan Type*(*s*)][*Options*]{*target specification*}.

Fig. 3 shows the result of scanning the AP utility NMAP, performed by the attacking computer present in the same network.

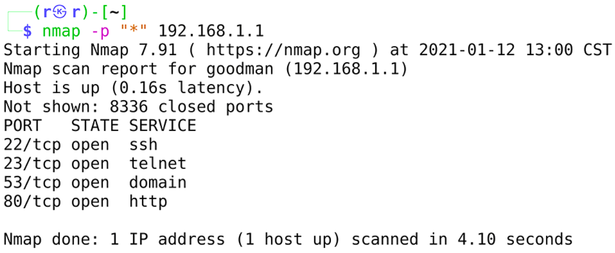
Active attacks. If the attacker has received enough information after a passive attack, they can launch an active attack [10]. There are quite a number of active attacks that are carried out in wireless networks [12]. They are carried out in order to implement:

- simulation of the connection (Spoofing);
- unauthorized access (access to files; deleting, modifying and adding data);
- Denial of Service DoS;
- introduction of malicious software.

Active attacks on wireless networks can be divided into three main categories:

- availability attacks;
- spoofing attacks;
- MITM (Man-In-The-Middle) attacks.

Availability attacks. Availability attacks are aimed at blocking the access of authorized users to wireless network resources. The attacker overloads the device with traffic and data until the device stops its normal operation. An attacker in a WLAN can easily carry out availability attacks, commonly referred to as Denial of Service (DoS) attacks [2, 13] or flooding [14]. These attacks target either specific network clients or AP. To carry out this attack, the attacker selects the victim's device and fills it with a huge number of packets via any of the network protocols. As a result, it becomes impossible to transfer data.



```
┌──(r㉿r)-[~]
└─$ nmap -p "*" 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-12 13:00 CST
Nmap scan report for goodman (192.168.1.1)
Host is up (0.16s latency).
Not shown: 8336 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.10 seconds
```

Fig. 3. The result of scanning ports with the NMAP utility

Table 1

Reconnaissance attacks

Type	Attacks	OSI level	Result
Reconnaissance attacks (Passive)	Eavesdropping	Physical	Interception of network traffic for further analysis
	Password Attacks	Data Link	Connecting to a wireless network, using its resources and carrying out other attacks on internal network nodes
	Port Scanning	Transport	Finding all open ports that can then be used to attack the target device

Table 2

Availability attacks

Type	Attacks	OSI level	Result
Availability attacks (Active)	Deauthentication attack	Data Link	Disconnection of legitimate clients from the AP which makes any data transfer impossible
	Disassociation attack		
	Authentication Request Flooding Attack		Exhaustion of AP resources, causing overflow of the customer association table. Unable to use local wireless network through the attacked AP
	CTS/RTS flood		Blocking data transfer
	Beacon flood		Creating non-existent ESSID. Overflow of the list of available networks, which will make it difficult for end users to find the desired network
	Probe Request)/Probe Response		Blocking data transfer between client and AP
	SYN/ACK flood	Transport	Violation of connection of legitimate clients to the server
	Block ACK flood		Blocking data transfer (attack is effective against 802.11n networks)

Deauthentication attack. The deauthentication attack can be carried out by devices that are not connected to the network, but are within range of this wireless network. During an attack, an attacker sends a lot of deauthentication frames in a very short period of time.

In [15], the authors researched and implemented a scenario of a deauthentication attack, during which a legitimate client was disconnected from the AP, which made any data transfer impossible.

Disassociation attack. The disassociation attack is very similar to the deauthentication attack in terms of methodology, simplicity of execution, and effect [16]. In this case, the attacker sends a disassociation message. Theoretically, such an attack is less effective because the client needs fewer procedures to return to the connection state. In this way, the duration of the connection loss is shorter.

Authentication Request Flooding Attack. During this attack, the attacker tries to deplete the AP's resources, causing the client association table to overflow. As a result of the overflow, it will not be possible to use the wireless LAN through the attacked AP. This attack is based on the fact that the maximum number of clients contained in the association table is limited and depends either on the hard value set in the access point settings or on the limitations of the physical memory. An entry of the access point in the client association table appears after receiving an authentication request message, even if the client does not complete its authentication (i.e. still in a state of unrecognized or unassociated).

Typically, an attacker must emulate a large number of fake clients and simply send an authentication frame on behalf of everyone. Once the AP client association table is full of fake records, the AP will no longer be able to associate stations (STA). This attack was described in more detail and studied in [1].

CTS/RTS flood attack. A pair of Request to Send (RTS) and Clear to Send (CTS) messages is an optional RF access control mechanism. In a CTS flood attack, an attacker may constantly transmit CTS frames to himself or another STA, thereby forcing other STAs on the network to permanently delay their transmission.

RTS-flood attack also uses the RTS/CTS, but it works the opposite way compared to the CTS-flood. An attacker transmits a large number of counterfeit RTS frames with possibly a longer transmission duration window, hoping to monopolize the wireless environment in such a way that it will eventually force other STAs to refuse transmission.

In [17] a detailed analysis of CTS and RTS attacks is presented, their impact on network performance and countermeasures.

Beacon flood attack. This is a form of DoS attack that an attacker can use in two different ways – to annoy network users or complete refusal to connect new customers.

In the first case, the attacker will transmit a constant stream of the fake Beacon frames that provide non-existent ESSIDs. This will overflow the list of available networks, which will make it difficult for end users to find the desired network. In the second case, the attacker will transmit a stream of the fake Beacon frames with a specific ESSID that corresponds to different (non-existent) BSSIDs. As a result, customers will constantly check whether each of the synonyms ESSID corresponds to the existing network.

Probe Request/Probe Response attacks. These attacks are intended to restrict access point resources and ultimately to block its operation. According to the 802.11 standard, the access point is obliged to respond to each request (Probe Request) with a special message – response (Probe Response) [18]. Such messages contain information about the network and access point capabilities. An attacker could send a steady stream of fake Probe Request packets. If this is done on a large scale and over a long period of time, the AP will not be able to afford to serve its true customers.

The Probe Response attack also uses the mechanism of Probe-requests and Probe-responses, and works the other way around, targeting the client rather than the access point. In this case, the attacker monitors the messages of Probe-requests coming from real customers and, acting as an access point, transmits to STA a stream of false and incorrect Probe-responses. These messages contain dummy network information, thus misleading the STA, which cannot receive a response from the genuine AP and then connect to any other AP.

SYN/ACK flood attack. According to the process of "triple handshake" of the TCP protocol in Fig. 4, the client sends a packet with the SYN flag (Synchronize). In response, the server must respond with a combination of flags SYN + ACK (Acknowledges). The client must then respond with a packet with an ACK flag, after which the connection is considered to be established.

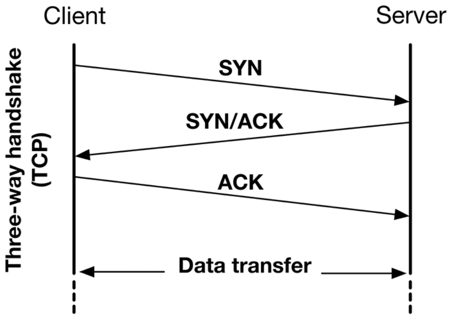


Fig. 4. Procedure for establishing a TCP connection

The principle of the attack is that the attacker, sending SYN requests, overflows on the server queue for connection. It ignores SYN + ACK server packets without sending response packets, or forges the packet header so that the SYN+ACK response packet is sent to a non-existent address. In the queue of connections there are so-called Half open connections, which are waiting for confirmation from the client. After a certain waiting time, these connections are discarded. The attacker's task is to keep the queue full to prevent new connections. Because of this, legitimate customers will not be able to establish a connection, or establish it with significant delays.

The article [19] shows in detail the types of SYN-flood attacks and presents effective algorithms for detecting anomalies of these attacks.

Block ACK flood. By performing this attack, an attacker can force the AP to voluntarily reject all packets received from the legitimate client, as a result of which the client will not be able to transmit data over the wireless network. The attack is effective against 802.11n networks and uses the mechanism of Add Block Acknowledgment – ADDBA, presented in this version of the standard. This mechanism allows the client to simultaneously transmit one large block of frames instead of several smaller segments. The ADDBA message must be sent on behalf of the client to notify the AP of its intention to fulfill such a request. This message contains information such as block size and corresponding sequence numbers. After receiving such a message, the access point will accept only those frames that fall into the specified sequence, and discard others.

To carry out this attack, the attacker simply needs to falsify the ADDBA frame, which has the client's MAC address and large sequence numbers. All traffic transmitted by the client will be ignored until the sequence numbers specified in the inadmissible ADDBA frame are reached. This attack is difficult to detect because it is effective even when introducing extremely low amounts of traffic into the network. Also, the attacker should not be present throughout the attack [20].

Spoofing attacks. Attempting to change your assigned MAC address with malicious intent is called a forgery MAC address, which is the main technique of MAC-attacks.

Each network node is equipped with a network interface controller (NIC) and has a unique MAC address that is used for user authentication [6]. By performing an eavesdropping attack, an attacker can steal the MAC address of a legitimate node. Though the MAC address is hard-coded in the network node's network card, it can be forged. Thus, the substitution of the MAC address allows a malicious node to hide its true identity or impersonate another network node in order to commit illegal acts.

ARP Poisoning. Address Resolution Protocol (ARP) is a standard protocol that maps a device's logical address to the physical address of that device. Each time a device wants to know the MAC address of another device, it transmits an ARP request to the network with the IP address of this device, and the device with the specified IP address responds and reports its MAC address [21]. Address Resolution Poisoning (ARP) is an attack that involves sending fake ARP messages over a local area network. These attacks try to redirect traffic from the originally planned host to the attacker. ARP poisoning is a type of attack that can be used to stop, change, or intercept network traffic. The technique is often used to initiate further offensive actions, such as session interception or denial of service [22].

Table 3

Spoofing attacks

Type	Attacks	OSI level	Result
Spoofing attacks (Active)	ARP Poisoning (ARP Spoofing)	Network	Redirecting traffic of victim devices through the attacker's computer
	MAC address spoofing	Data Link	MAC address forgery
	DNS Spoofing	Application	Redirecting the victim's traffic to the attacker's computer

When attacking ARP poisoning occurs, the malicious device sends a fake ARP request to the victim's device. The device-victim responds and sends its MAC address.

MAC address spoofing. MAC-address spoofing is an attack that is often used to connect to a router with MAC address filtering or for the purpose of preventing the possibility of proving the involvement of an attacker in illegal actions. In this attack, an attacker monitors devices connected to the network using monitoring mode, clones the MAC address and uses it for his wireless network adapter.

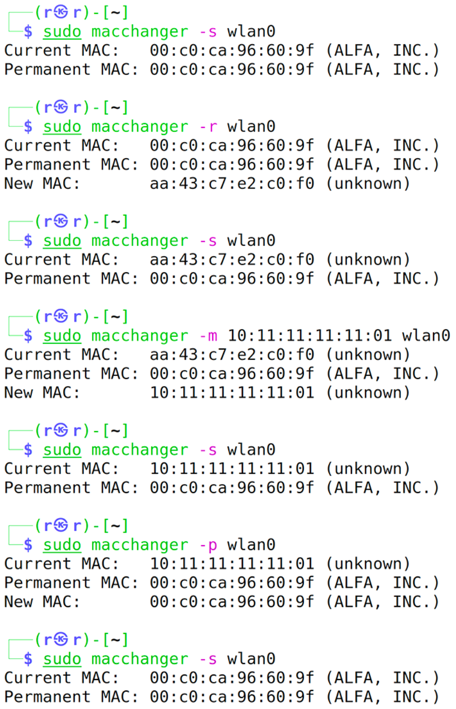
To demonstrate MAC address spoofing, we used macchanger utility from OS Kali Linux software package. This program offers various functions, such as changing the address so that it corresponds to a particular manufacturer, or its complete randomization.

DNS Spoofing. DNS stands for Domain Name System, and the main use of this server is to translate domain names into appropriate IP addresses. DNS spoofing is a type of attack, the principle of which is based on the falsification of DNS records in order to redirect traffic to a fake Internet site. For example, an attacker can deploy a copy of facebook.com on their server, and whenever the victim's device tries to go to the original facebook.com page, it is redirected to the attacker's computer, where the attacker collects the credentials of unsuspecting users, Fig. 6.

An example of implementing a DNS spoofing attack using the Kali Linux OS is shown in [23].

MITM attacks. In addition to the aforementioned MAC spoofing and identity theft attacks, the MAC-level attack class also includes MITM attacks. An attacker disguises himself or herself as one of the network nodes in order to obtain information addressed to the node, the imitation of which is carried out.

Attacks of this class lead to a serious breach of network security, as they allow unauthorized or malicious users to gain full access to information transmitted over the network.



```
┌──(r㉿r)-[~]
└─$ sudo macchanger -s wlan0
Current MAC:   00:c0:ca:96:60:9f (ALFA, INC.)
Permanent MAC: 00:c0:ca:96:60:9f (ALFA, INC.)

┌──(r㉿r)-[~]
└─$ sudo macchanger -r wlan0
Current MAC:   00:c0:ca:96:60:9f (ALFA, INC.)
Permanent MAC: 00:c0:ca:96:60:9f (ALFA, INC.)
New MAC:       aa:43:c7:e2:c0:f0 (unknown)

┌──(r㉿r)-[~]
└─$ sudo macchanger -s wlan0
Current MAC:   aa:43:c7:e2:c0:f0 (unknown)
Permanent MAC: 00:c0:ca:96:60:9f (ALFA, INC.)

┌──(r㉿r)-[~]
└─$ sudo macchanger -m 10:11:11:11:11:01 wlan0
Current MAC:   aa:43:c7:e2:c0:f0 (unknown)
Permanent MAC: 00:c0:ca:96:60:9f (ALFA, INC.)
New MAC:       10:11:11:11:11:01 (unknown)

┌──(r㉿r)-[~]
└─$ sudo macchanger -s wlan0
Current MAC:   10:11:11:11:11:01 (unknown)
Permanent MAC: 00:c0:ca:96:60:9f (ALFA, INC.)

┌──(r㉿r)-[~]
└─$ sudo macchanger -p wlan0
Current MAC:   10:11:11:11:11:01 (unknown)
Permanent MAC: 00:c0:ca:96:60:9f (ALFA, INC.)
New MAC:       00:c0:ca:96:60:9f (ALFA, INC.)

┌──(r㉿r)-[~]
└─$ sudo macchanger -s wlan0
Current MAC:   00:c0:ca:96:60:9f (ALFA, INC.)
Permanent MAC: 00:c0:ca:96:60:9f (ALFA, INC.)
```

Fig. 5. Changing the MAC address of the wireless interface

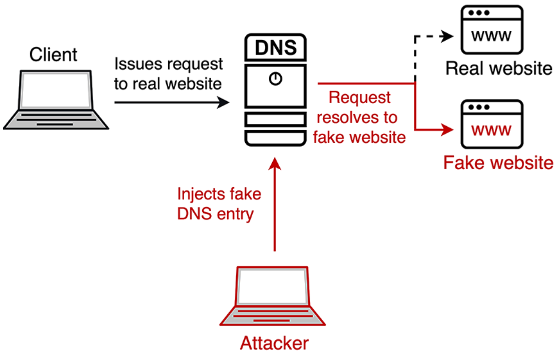


Fig. 6. DNS Spoofing

Table 4

MITM attacks

Type	Attacks	OSI level	Result
MITM attacks (Active)	ARP Spoofing	MultiLayer	Access to confidential information of network users, making any changes to its content, arbitrary regulation of network traffic flows
	"Evil Twin"		Replacement of the original AP, to which the user connects to the duplicate, which gives the attacker the ability to access confidential information

Accordingly, mediator attacks can occur at levels 1 to 7 and at each intermediate level.

In these attacks, the attacker is between the devices that exchange information.

ARP Spoofing. An example of a MITM attack is the previously discussed ARP Spoofing attack. This attack requires that the attacker be in the same network as the victim device. By gaining access to encryption keys and carrying out an ARP substitution attack, the attacker has the ability to listen to and intercept all important confidential information of network users, make any changes to its content, arbitrarily regulate network traffic flows.

This attack was carried out using the OS Kali Linux mitmf tool (Man-In-The-Middle-Framework).

Command to launch this attack is

$mitmf –arp –spoof –gateway<gateway ip>–targets<ips of target machines>-i<interface name>.

To launch this attack, an NMAP scan is first performed to find out the IP and MAC addresses of all devices, including the network gateway. As soon as an attacker obtains host addresses, they begin sending fake ARP packets over the local network to the hosts. Fraudulent messages inform recipients that the attacker's MAC address must be associated with the IP address of the device it is targeting. The ARP table entries on the victim device before and after the attack are shown in Fig. 8.

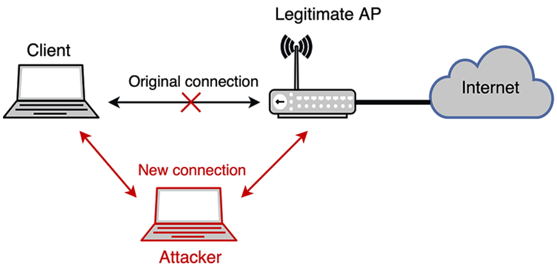
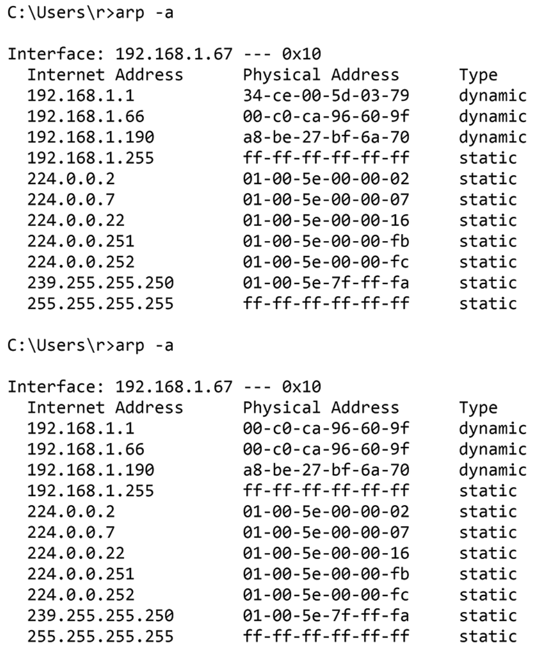


Fig. 7. Man-in-the-Middle (MITM) attack


```
C:\Users\r>arp -a

Interface: 192.168.1.67 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           34-ce-00-5d-03-79     dynamic
  192.168.1.66          00-c0-ca-96-60-9f     dynamic
  192.168.1.190         a8-be-27-bf-6a-70     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.7             01-00-5e-00-00-07     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\r>arp -a

Interface: 192.168.1.67 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           00-c0-ca-96-60-9f     dynamic
  192.168.1.66          00-c0-ca-96-60-9f     dynamic
  192.168.1.190         a8-be-27-bf-6a-70     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.7             01-00-5e-00-00-07     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Fig. 8. ARP table entries on the victim device before and after the attack

"Evil Twin" attack. An Evil Twin is setting up a rogue access point (RAP) by cloning the MAC address and service set ID of an existing wireless AP. Such access points are possible because the 802.11 standard allows the existence of multiple access points with the same ESSID in the same area.

The purpose of the Evil Twin attack is to deceive users and force them to unknowingly connect to the RAPs under the guise that they are connected to a legitimate access point. Initially, an attacker creates a fake access point (usually implemented in software) that broadcasts an ESSID similar to that of a legitimate AP operating nearby. If the network adapter (Network Interface Card – NIC) transmits an attacker with a stronger signal, the client will prefer to connect to such a fake network. Once a customer is connected, an attacker eavesdrops on his messages, can redirect customers to malicious websites, steal customer credentials, and more.

It should be noted that the "Evil Twin" must provide an Internet connection for customers who connect to it. To provide the Internet, an Evil Twin can establish a connection using a legitimate access point, as shown in Fig. 7 (because the legitimate AP is already configured to provide Internet services), or the Evil Twin can provide a private Internet connection by itself, as shown in Fig. 9. An attacker's private connection helps him or her to overcome many existing detection methodologies.

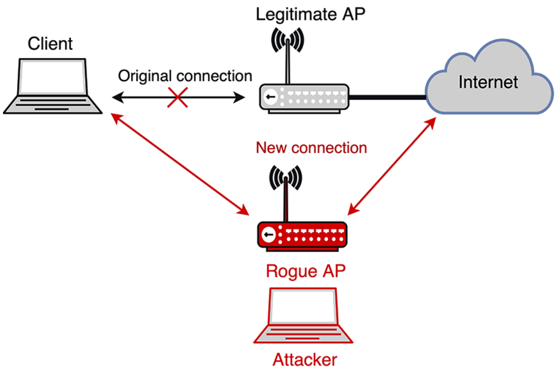


Fig. 9. "Evil Twin" attack

Conclusions. The results of the study showed that the current protocols do not provide a complete solution to WLAN security issues for attacks by both external and internal attackers. It is established that passive attacks aimed at reconnaissance operations in most cases do not cause deviations in the operation of the WLAN from the normal mode. In turn, active attacks, where any intrusion is characterized by certain features, can be described as some deviation from the normal behavior of WLAN. When analyzing attacks at the appropriate levels of the OSI network model and determining the destructive consequences of their implementation, it was found that in addition to attacks that violate only one level of OSI, man-in-the-middle attacks use several levels of the network model. This allows attackers to gain full access to information transmitted over the network. It should also be noted that, to ensure the security of WLAN requires a comprehensive approach that takes into account the attacks at different levels of the OSI network model. Further research should focus on finding and developing the best security solutions and methods for WLAN.

References.

1. Singh, R., & Sharma, T. P. (2014). On the IEEE 802.11i security: a denial-of-service perspective. *Security and Communication Networks, 8*(7), 1378-1407. https://doi.org/10.1002/sec.1079.

2. Farooq, T., Llewellyn-Jones, D., & Merabti, M. (2010). MAC Layer DoS Attacks in IEEE 802.11 Networks. *The 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010)*, Liverpool, UK. Retrieved from http://www.cms.livjm.ac.uk/pgnet2010/MakeCD/Papers/2010063.pdf.

3. Singh, P., Mishra, M., & Barwal, P. N. (2014). Analysis of security issues and their solutions in wireless LAN. *International Conference on Information Communication and Embedded Systems* (*ICICES2014*), 1-6. https://doi.org/10.1109/icices.2014.7033871.

4. Aung, M., & Thant, K. (2019). IEEE 802.11 Attacks and Defenses. *Seventeenth International Conference on Computer Applications* (*ICCA 2019*), 186-191. Retrieved from https://meral.edu.mm/record/3457/files/ICCA%202019%20Proceedings%20Book-pages-197-202.pdf.

5. Waliullah, M., & Gan, D. (2014). Wireless LAN Security Threats & Vulnerabilities. *International Journal of Advanced Com-puter Science and Applications, 5*(1), 176-183. https://doi.org/10.14569/ijacsa.2014.050125.

6. 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. https://doi.org/10.1109/jproc.2016.2558521.

7. Li, Y., Li, D., Cui, W., & Zhang, R. (2011). Research based on OSI model. *2011 IEEE 3rd International Conference on Communication Software and Networks*, 554-557. https://doi.org/10.1109/iccsn.2011.6014631.

8. Martinović, M., Lovaković, D., & Ćosić, T. (2014). Network Security Issues in Regard to OSI Reference Model Layers. U: Major, A. (ur.) *Proceedings of TEAM 2014: 6th International Scientific and Expert Conference of the International TEAM Society*, 105-107. Retrieved from http://www.teamsociety.org/_Data/Files/140207115235606.pdf.

9. Cheng, M., Ling, Y., & Wu, W. B. (2017). Time Series Analysis for Jamming Attack Detection in Wireless Networks. *GLOBECOM 2017 – 2017 IEEE Global Communications Conference*, 1-7. https://doi.org/10.1109/glocom.2017.8254000.

10. Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics, 9*(7), 1177. https://doi.org/10.3390/electronics9071177.

11. Chang, T.-H., Chen, C.-M., Hsiao, H.-W., & Lai, G.-H. (2018). Cracking of WPA & WPA2 Using GPUs and Rule-based Method. *Intelligent Automation and Soft Computing*, 183-192. https://doi.org/10.31209/2018.100000054.

12. Sabillon, R., Cano M., Jeimy, Serra-Ruiz, Jordi & Cavaller, Víctor (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security, 4*, 165-176.

13. Buriachok, V., & Sokolov, V. (2018). Using 2.4 GHz Wireless Botnets to Implement Denial-of-Service Attacks. *International Academy Journal Web of Scholar24*, 14–21. https://doi.org/10.31435/rsglobal_wos/12062018/5734.

14. Mahrach, S., & Haqiq, A. (2020). DDoS Flooding Attack Mitigation in Software Defined Networks. *International Journal of Advanced Computer Science and Applications, 11*(1), 693-700. https://doi.org/10.14569/ijacsa.2020.0110185.

15. Kristiyanto, Y., & Ernastuti Ernastuti (2020). Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test. *CommIT (Communication and Information Technology) Journal, 14*(1), 45-51. https://doi.org/10.21512/commit.v14i1.6337.

16. Cheema, R., Bansal, D., & Sofat, S. (2011). Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks. *International Journal of Computer Applications, 23*(7), 7-15. https://doi.org/10.5120/2901-3801.

17. Sawwashere, S. S., & Nimbhorkar, S. U. (2014). Survey of RTS-CTS Attacks in Wireless Network. *2014 Fourth International Conference on Communication Systems and Network Technologies*, 752-755. https://doi.org/10.1109/csnt.2014.158.

18. Ratnayake, D. N., Kazemian, H. B., Yusuf, S. A., & Abdullah, A. B. (2011). An Intelligent Approach to Detect Probe Request Attacks in IEEE 802.11 Networks. *Engineering Applications of Neural Networks*, 372-381. https://doi.org/10.1007/978-3-642-23957-1_42.

19. Bogdanoski, M., Shuminoski, T., & Risteski, A. (2013). Analysis of the SYN Flood DoS Attack. *International Journal of Computer Network and Information Security, 5*(8), 15-11. https://doi.org/10.5815/ijcnis.2013.08.01.

20. Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2016). Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset. *IEEE Communications Surveys & Tutorials, 18*(1), 184-208. https://doi.org/10.1109/comst.2015.2402161.

21. Nenovski, B., & Mitrevski, P. (2015). Real-World ARP Attacks and Packet Sniffing, Detection and Prevention on Windows and Android Devices. *Conference on Informatics and Information Technology 2015*, (pp. 186-191). Retrieved from http://ciit.finki.ukim.mk/data/papers/CiitFinal2015.pdf.

22. Lake, J. (n.d.). *ARP poisoning/spoofing: How to detect & prevent it*. Retrieved from https://www.comparitech.com/blog/vpn-privacy/arp-poisoning-spoofing-detect-prevent/.

23. Cisar, P., & Pinter, R. (2019). Some ethical hacking possibilities in Kali Linux environment. *Journal of Applied Technical and Educational Sciences, 9*(4), 129-149. https://doi.org/10.24368/jates.v9i4.139.

Аналіз атак у мережах IEEE 802.11 на різних рівнях моделі OSI

Р. Ю. Корольков, С. В. Куцак

Національний університет «Запорізька політехніка», м. Запоріжжя, Україна, e-mail: romankor@zntu.edu.ua

Мета. Аналіз основних типів уразливостей і визначення слабких місць у безпеці безпроводових мереж 802.11, виявлення причин втрати інформації або порушення функціонування мережі в результаті атак.

Методика. Дослідження атак на різних рівнях мережної моделі OSI.

Результати. Визначені основні загрози і атаки, що реалізуються на кожному окремому рівні мережної моделі

OSI, від фізичного до прикладного рівня. Розглянуто 15 різних атак з детальним описом наслідків їх реалізації. Встановлена відповідність між рівнями мережної моделі OSI та особливостями реалізації атак.

Наукова новизна. Застосовано принцип підвищення рівня абстракції для систематизації атак на WLAN. По-перше, зіставлені відомі атаки за рівнями мережної моделі OSI та вказані деструктивні наслідки їх реалізації, по-друге, виділені чотири типи атак (рекогносцирування, доступності, підміни, посередника), по-третє, атаки розділені на категорії пасивних і активних. Такий підхід дає можливість отримати більш концептуальне розуміння проблем безпеки безпроводових мереж.

Практична значимість. Отримані результати можуть бути використані для розробки ефективних багаторівневих систем виявлення й запобігання вторгнень у WLAN.

Ключові слова: *атака, безпроводова мережа, мережний рівень, спуфінг, точка доступу*

Анализ атак в сетях IEEE 802.11 на разных уровнях модели OSI

Р. Ю. Корольков, С. В. Куцак

Национальный университет «Запорожская политехника», г. Запорожье, Украина, e-mail: romankor@zntu.edu.ua

Цель. Анализ основных типов уязвимостей и определение слабых мест в безопасности беспроводных сетей 802.11, выявление причин потери информации или нарушения функционирования сети в результате атак.

Методика. Исследование атак на разных уровнях сетевой модели OSI.

Результаты. Определены основные угрозы и атаки, реализуемые на каждом отдельном уровне сетевой модели OSI, от физического до прикладного уровня. Рассмотрено 15 различных атак с подробным описанием последствий их реализации. Установлено соответствие между уровнями сетевой модели OSI и особенностями реализации атак.

Научная новизна. Применен принцип повышения уровня абстракции для систематизации атак на WLAN. Во-первых, сопоставлены известные атаки уровням сетевой модели OSI и указаны деструктивные последствия их реализации, во-вторых, выделено четыре типа атак (рекогносцировки, доступности, подмены, посредника), в-третьих, атаки разделены на категории пассивных и активных. Такой подход дает возможность получить более концептуальное понимание проблем безопасности беспроводных сетей.

Практическая значимость. Полученные результаты могут быть использованы для разработки эффективных многоуровневых систем обнаружения и предотвращения вторжений в WLAN.

Ключевые слова: *атака, беспроводная сеть, сетевой уровень, спуфинг***,** *точка доступа*

Recommended for publication by L. M. Karpukov, Doctor of Technical Science. The manuscript was submitted 23.10.20.