DOI: 10.26565/2304-6201-2021-50-06

UDC 004.056.53

Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection

R. Korolkov, S. Kutsak, V. Voskoboinyk

Korolkov Roman *Senior Lecturer of the Information Security Department*
National University "Zaporizhzhia Polytechnic", Zhukovsky St., 64, Zaporizhzhia, 69063, Ukraine
e-mail: romankor@zntu.edu.ua;
https://orcid.org/0000-0001-5501-4600

Kutsak Serhii *Senior Lecturer of the Information Security Department*
National University "Zaporizhzhia Polytechnic", Zhukovsky St., 64, Zaporizhzhia, 69063, Ukraine
e-mail: kutsaksv@zntu.edu.ua;
https://orcid.org/0000-0001-5238-8957

Voskoboinyk Volodymyr *PhD, Professor of the Information Security Department*
National University "Zaporizhzhia Polytechnic", Zhukovsky St., 64, Zaporizhzhia, 69063, Ukraine
e-mail: wskva2018@gmail.com;
https://orcid.org/0000-0003-3786-8666

The issues related to IEEE 802.11 technology are considered in the article. The vulnerability that allows an attacker to perform a deauthentication attack is described in detail. Analysis and practical experiments have shown that the existing vulnerability of Wi-Fi technology presents danger to legitimate users, and by using it, an attacker can send deauthentication frames, which results in disrupting communication between clients and the access points to which they are connected. Kali Linux OS, Aircrack-ng tool to launch attacks and Wireshark to capture and analyze IEEE 802.11 frames has been used for research. Our experimental studies helped to identify the anomalies during the attack and the algorithm for detecting deauthentication attacks based on those anomalies has been developed. The proposed solution uses a combination of three parameters (reason code, timestmap, RSSI signal strength level), which in our opinion can reduce the frequency of false positives. It is proposed to use the DDA (Detector of Deauthentication Attack) to scan and analyze wireless traffic, and issue warnings if an attack is detected.

Keywords: *attack, deauthentication, injection of packets, connection, access point, frame, DoS, Linux, Wi-Fi.*

Аналіз атаки деавтентифікації в мережах IEEE 802.11 та пропозиція по її виявленню

Р.Ю. Корольков, С.В. Куцак, В.О. Воскобойник

Корольков Роман Юрійович *старший викладач кафедри "Захист інформації"*
Національний університет "Запорізька політехніка", вул. Жуковського, 64, м. Запоріжжя, 69063, Україна

Куцак Сергій Вікторович *старший викладач кафедри "Захист інформації"*
Національний університет "Запорізька політехніка", вул. Жуковського, 64, м. Запоріжжя, 69063, Україна

Воскобойник Володимир Олександрович *к.т.н., професор кафедри "Захист інформації"*
Національний університет "Запорізька політехніка", вул. Жуковського, 64, м. Запоріжжя, 69063, Україна

Безпроводові мережі використовують радіоефір та широкомовну природу фізичного рівня і через це надзвичайно вразливі до можливих атак і несанкціонованого доступу. У статті розглянуті питання, пов'язані з технологією IEEE 802.11, докладно описана вразливість, яка дозволяє зловмиснику виконувати DoS-атаку у ситуації, коли не використовуються захищені кадри управління Protected Management Frames (PMF). Аналіз і практичні експерименти

довели, що існуюча вразливість технології Wi-Fi до сих пір залишається небезпечною для кінцевих користувачів, і використовуючи її зловмисник може відправляти підроблені кадри деавтентифікації, що призводить до порушення зв'язку між клієнтами та точками доступу, до яких вони підключені. Дану атаку реалізовано на реальному випробувальному стенді безпроводової мережі і проведені обширні експерименти по вивченню поведінки мережних вузлів в нормальних умовах та під час атаки. Для реалізації атаки були використані: операційна система Kali Linux, інструмент Aircrack-ng для запуску атаки і Wireshark для захоплення і аналізу кадрів IEEE 802.11. Експериментальні дослідження дозволили виділити аномалії під час атаки і на підставі цього запропоновано алгоритм виявлення атак деавтентифікації. Пропонується використовувати детектор атаки деавтентифікації (Detector of Deauthentication Attack DDA), який буде сканувати та аналізувати безпроводовий мережний трафік, і видавати попередження у разі виявлення атаки. Запропоноване рішення використовує комбінації з трьох параметрів (код причини reason code, часова мітка timestmap, рівень потужності сигналу RSSI), що на наш погляд дозволить знизити частоту помилкових спрацьовувань.

Ключові слова: *атака, деавтентифікація, ін'єкція пакетів, підключення, точка доступу, кадр, DoS, Linux, Wi-Fi.*

Анализ атаки деаутентификации в сетях IEEE 802.11 и предложение по ее обнаружению

Корольков Роман Юрьевич *старший преподаватель кафедры "Защита информации" Национальный университет "Запорожская политехника", ул. Жуковского, 64, г. Запорожье, 69063, Украина*

Куцак Сергей Викторович *старший преподаватель кафедры "Защита информации" Национальный университет "Запорожская политехника", ул. Жуковского, 64, г. Запорожье, 69063, Украина*

Воскобойник Владимир Александрович *к.т.н., профессор кафедры "Защита информации" Национальный университет "Запорожская политехника", ул. Жуковского, 64, г. Запорожье, 69063, Украина*

В статье рассмотрены вопросы, связанные с технологией IEEE 802.11, подробно описана уязвимость, которая позволяет злоумышленнику выполнять DoS-атаку в ситуации, когда не используются защищенные кадры управления Protected Management Frames (PMF). Анализ и практические эксперименты показали, что существующая уязвимость технологии Wi-Fi до сих пор остается опасной для конечных пользователей, и используя ее злоумышленник может отправлять поддельные кадры деаутентификации, что приводит к нарушению связи между клиентами и точками доступа, к которым они подключены. Данную атаку реализовано на реальном испытательном стенде беспроводной сети и проведены обширные эксперименты по изучению поведения сетевых узлов в нормальных условиях и во время атаки. Для реализации атаки были использованы: операционная система Kali Linux, инструмент Aircrack-ng для запуска атаки и Wireshark для захвата и анализа кадров IEEE 802.11. Экспериментальные исследования позволили выделить аномалии во время атаки и на основании этого предложен алгоритм обнаружения атак деаутентификации. Предлагается использовать детектор атаки деаутентификации (Detector of Deauthentication Attack DDA), который будет сканировать и анализировать беспроводной сетевой трафик, и выдавать предупреждения в случае обнаружения атаки. Предложенное решение использует комбинации из трех параметров (код причины reason code, временная метка timestmap, уровень мощности сигнала RSSI), что на наш взгляд позволит снизить частоту ложных срабатываний.

Ключевые слова: атака, деаутентификация, инъекция пакетов, подключение, точка доступа, кадр, DoS, Linux, Wi-Fi.

1 Introduction

IEEE 802.11 wireless networks have become one of the most widely used networks because it is supported by an extremely large number of devices, such as smartphones, laptops, tablets, IoT devices, etc. Unlike cable networks, where the interception of transferred information is impossible without physical access, wireless networks are vulnerable to unauthorized access and possible attacks, unless special measures are taken [1]. The passive access is natural for the wireless networks. Attackers can easily target wireless devices because the Wi-Fi network cannot prevent "listening" to transmitted traffic, as well as possibility to intercept and analyze packets. Therefore, an attacker can intercept information or attack the system with impunity.

Wi-Fi vulnerabilities and IEEE 802.11 security methods have been studied for a long time. Nevertheless, the issue of security has not become less important and ongoing research into the vulnerabilities of the IEEE 802.11 standard is necessary to prevent future transgressions.

A deauthentication attack, being one type of attack, which Wi-Fi networks are prone to, due to the shortcomings of the IEEE 802.11 protocols [2] is discussed in this article. A deauthentication attack is a denial-of-service (DoS) attack for one or more users and falls under the Management frame attack

category. The management frames are important system data packets that are used to control the communication of stations and access points [3].

Fig. 1.1 shows the frame structure of the IEEE 802.11 protocol at the MAC level. The critical part of the frame is "MAC Header and Data".

There are three types of frame:

1. Management frames (type 00)
2. Control frames (type 01)
3. Data frames (type 10)

The management frames are responsible for ensuring the interaction between the access point and the wireless clients and can be divided into subtypes (determined by the 4-bit value of the "SubType" field). These subtypes are responsible for the initial interactive operations between clients and access points.

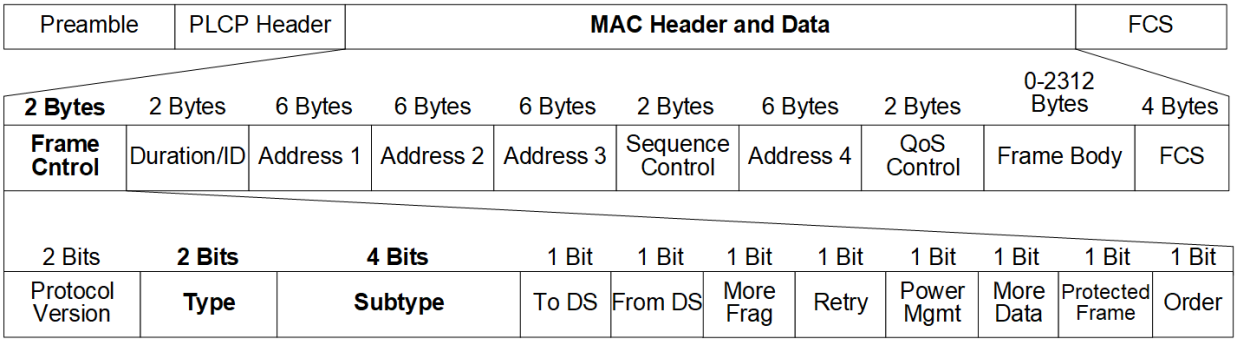

Fig.1.1 802.11 frame structure

The list of 12 subtypes of management frames defined by 802.11 standards is given in Tab. 1.

Table 1. Subtypes of the management frame

Type	Description	Subtype	Description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1111	Reserved

Control frames are responsible for ensuring the proper exchange of data between the access point and the wireless clients. Control frames have three subtypes: CTS, RTS, ACK and are used for the CSMA/CA mechanism.

Data frames contain actual data received from the network layer and are protected by security mechanisms such as WEP, WPA or WPA2.

Unfortunately, unlike data frames that are transmitted over the network in an encrypted form, management frames are not encrypted. Due to the lack of encryption, 802.11 management frames are vulnerable to various threats, including deauthentication attacks [4]. An attacker could exploit this vulnerability by falsifying the MAC address of devices, impersonating a client or access point (AP), and sending deauthentication requests [5]. The frames are accepted as coming from other device and the established connection is broken [6]. Therefore, a DoS attack is a critical attack that disrupts a client's current transactions. Thus, a mechanism to detect this attack needs developing.

The attacker falsifies the MAC address of the legitimate client and periodically sends deauthentication frames [5]. Authentication cancellation requests cannot be ignored, and the access point responds

immediately by canceling client authentication. After a successful attack, the client station disconnects from the wireless network and cannot reconnect until attack stops [6].

A specific channel can also be targeted by performing a DoS attack on multiple users simultaneously [13].

2 Problem statement

The deauthentication attack is considered to be one of the most powerful DoS attacks in the field of wireless communication, but it is also one of the most difficult to identify accurately. Therefore, the aim of the work is a practical study of the interaction between the client and the AP during the exchange of frames in normal conditions and during the DoS-attack.

To solve the problem, the following tasks have been set.

1. Practical implementation of a deauthentication attack.
2. Analysis of frames during the attack to identify anomalies.
3. Development of an algorithm for detecting deauthentication attacks.

3 Concept of deauthentication attack and its implementation

The IEEE 802.11 Wi-Fi standard requires two mandatory sequential steps before a user can begin data transfer: authentication and association [7]. Therefore, a Wi-Fi client can be in any of 3 states [8], and the communication process between the client and the access point can be described as follows:

state 0: the client is not authenticated and not associated;

The client searches for a network by sending a test request frame (Probe request) on several channels. The AP sends a Probe response to the client after receiving a Probe request. The client connects to the AP with the strongest signal. Authentication between the client and the access point is required to prevent illegal clients from accessing the network. Thus, the client sends an authentication request to the AP. The AP responds to the client by sending an authentication response with a status code.

state 1: the client is authenticated but not associated;

After authentication, the client sends an association request frame to the AP for access to the wireless network through the AP. The AP sends an association response to the client and stores the client information in its own database.

state 2: the client is authenticated and associated.

The connection is established and the client is able to send data to the access point and vice versa.

Once the authentication and association steps are successfully completed, the client and AP perform a four-way handshake to prove PSK knowledge and use it to obtain encryption keys. Afterwards encrypted data can be exchanged between devices [9].

The user's device sends a Wi-Fi deauthentication frame to another device to end a secure connection. The deauthentication frame is a notification, not a request [10]. After accepting the deauthentication message (whether counterfeit or genuine), a receiving party cannot refuse to execute it [11], unless frame protection mode is enabled (802.11w: MFP or Management Frame Protection). When the client receives the deauthentication frame, it goes directly to state 0, regardless of the current state.

An attacker could take advantage of this by forging this message and thereby breaking the connection between the wireless devices and their access point. Thus, the client targeted attacks reaches state 0 and requires re-authentication and re-association.

We have implemented a deauthentication attack on a real wireless test bench and analyzed the impact of the attack on the bandwidth, which reaches zero during the attack [6]. The test bench consists of a wireless network, an access point and a client. The AP is connected to the Internet, and the client connects to the AP. The AP provides all services to the connected client (Fig. 3.1).

The exchange of frames between the client and the access point during the connection and attack is shown in Fig. 3.1.

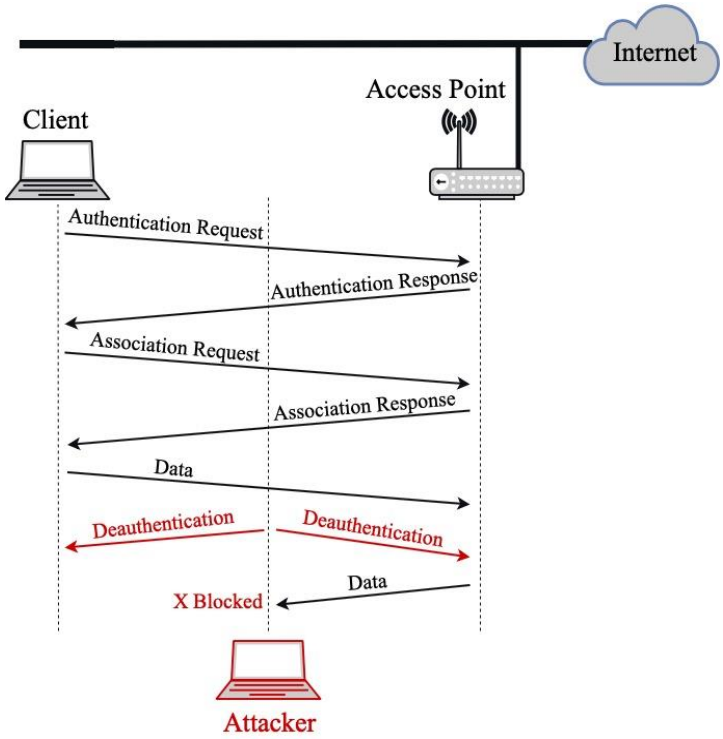

Fig.3.1 Deauthentication attack scenario

For our research, we used the Kali Linux OS and the Aircrack-ng tool to run a deauthentication attack. This tool has powerful utilities that can be used to put various wireless network cards in monitoring modes, as well as for packet injection [12].

The dual-band Wi-Fi adapter Alfa AWUS036ACH of 802.11ac standard on the Realtek RTL8812AU chipset with support for monitoring mode has been selected for the experiment.

The block diagram of the deauthentication attack algorithm is presented in Fig.3.2

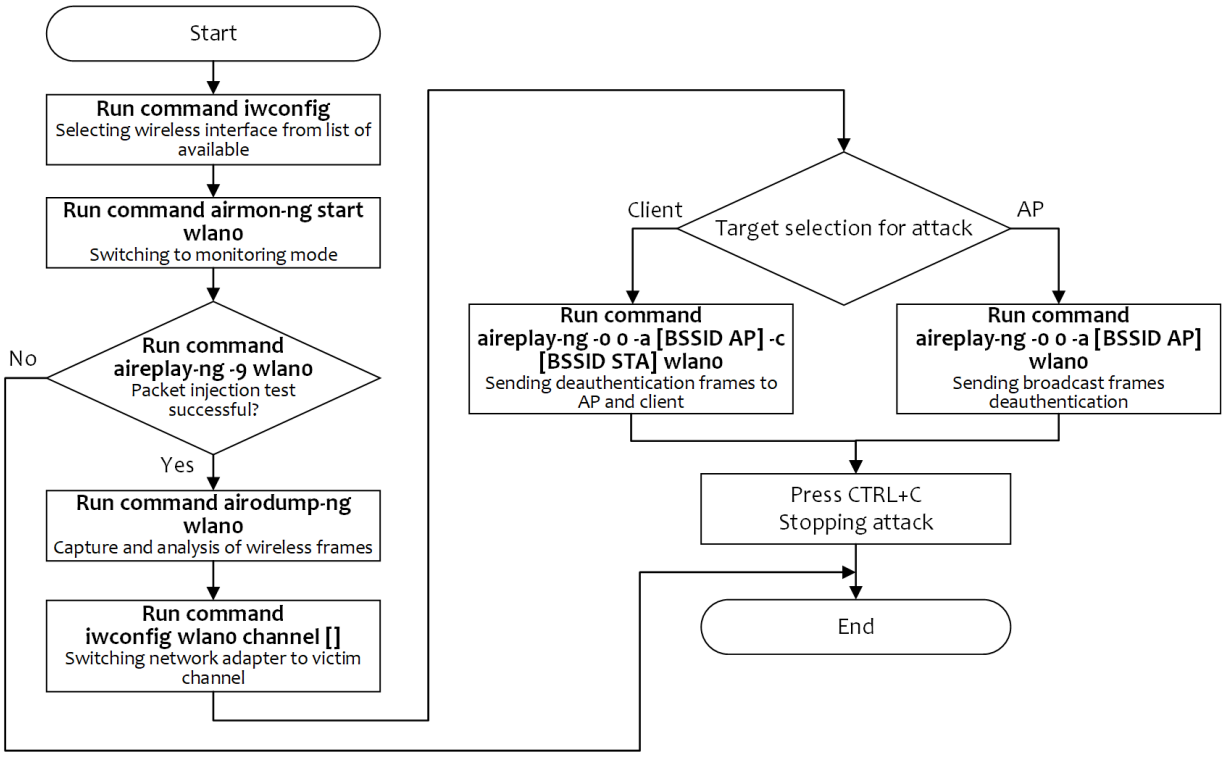

Fig.3.2 Block diagram of the deauthentication attack algorithm

The attacker spoofs a legitimate MAC-address of the client and sends periodic deauthentication frames [5]. Authentication cancellation requests cannot be ignored and the access point responds instantly to these requests by canceling client authentication. After a successful attack, the client station disconnects from the wireless network and cannot reconnect to it until the attacker stops the attack [6].

A particular channel could also be targeted to by performing DoS attack on multiple users simultaneously [13].

4. The frame analysis during a deauthentication attack

We have conducted extensive experiments to study the behavior of nodes both in normal conditions and during deauthentication attacks. A powerful Wireshark tool has been chosen to capture and analyze IEEE 802.11 frames.

Experimental studies have identified three anomalies during the attack of deauthentication.

4.1. Deauthentication frame flooding

Analysis of the deauthentication attack at the frame injection stage has shown that a successful attack requires the creation of a large number of deauthentication frames in a very short period of time. Fig. 4.1 shows the number of deauthentication broadcast frames sent by an attacker during an attack. The same type of observation has been made in the second case - a targeted attack on the client, as shown in Fig. 4.2.

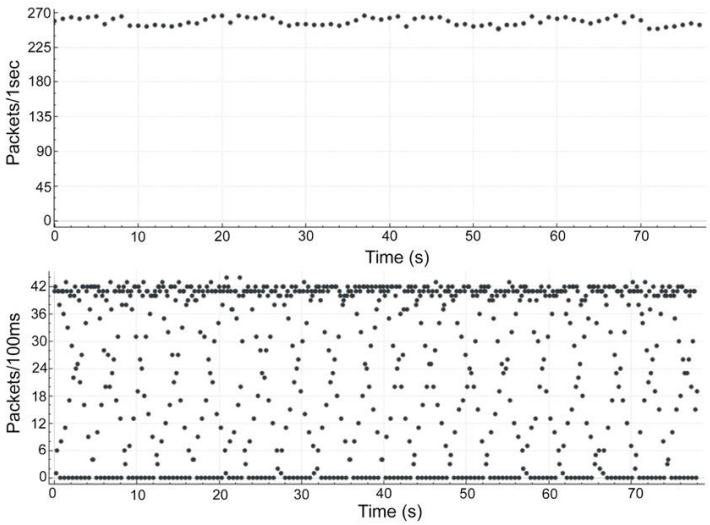

Fig.4.1 The distribution of deauthentication broadcast frames during the attack

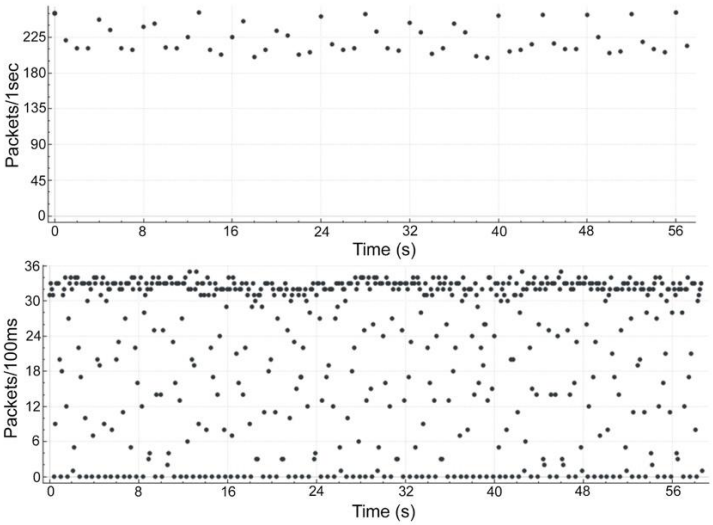

Fig.4.2 The distribution of deauthentication frames during a targeted attack on the client

The graphs show that there is a very small change in the time intervals between consecutive frames of deauthentication. In the case of a targeted attack on the client, the aireplay-ng command sends a total of 128 packets for each specified deauthentication message. 64 packets are sent to the AP, and 64 packets are sent to the client [6]. On average, 225-250 frames of deauthentication are sent by the program in 1 second, which is an anomaly, because it has been experimentally found that in 88% of cases, one deauthentication frame is enough to successfully complete a communication session [14].

4.2 Reason code for cancellation of authentication

The deauthentication frame contains the reason code, which explains why the connection is interrupted. Here are some of the common reason codes (Tab. 2) [15, 19].

Table 2. Reason codes for authentication cancellation

Code	Reason
0	Reserved
1	Unspecified reason
2	Previous authentication no longer valid
3	Station is leaving (or has left) IBSS or ESS
4	Disassociated due to inactivity
5	Disassociated because AP is unable to handle all currently associated stations
6	Class 2 frame received from nonauthenticated station
7	Class 3 frame received from nonassociated station
8	Disassociated because sending station is leaving (or has left) BSS
9	Station requesting (re)association is not authenticated with responding station
10	Disassociated because the information in the Power Capability element is unacceptable

Having analyzed the frames captured during the implementation of the attack by using the utility package Aircrack-ng, we have found that all frames of deauthentication have the reason code 7 (0x0007 Code 7) (Fig. 4.3), which has the following meaning: «Class 3 frame received from nonassociated station». We believe that the reason code 7 in the deauthentication frames may serve as an indicator of substitution deauthentication frames.

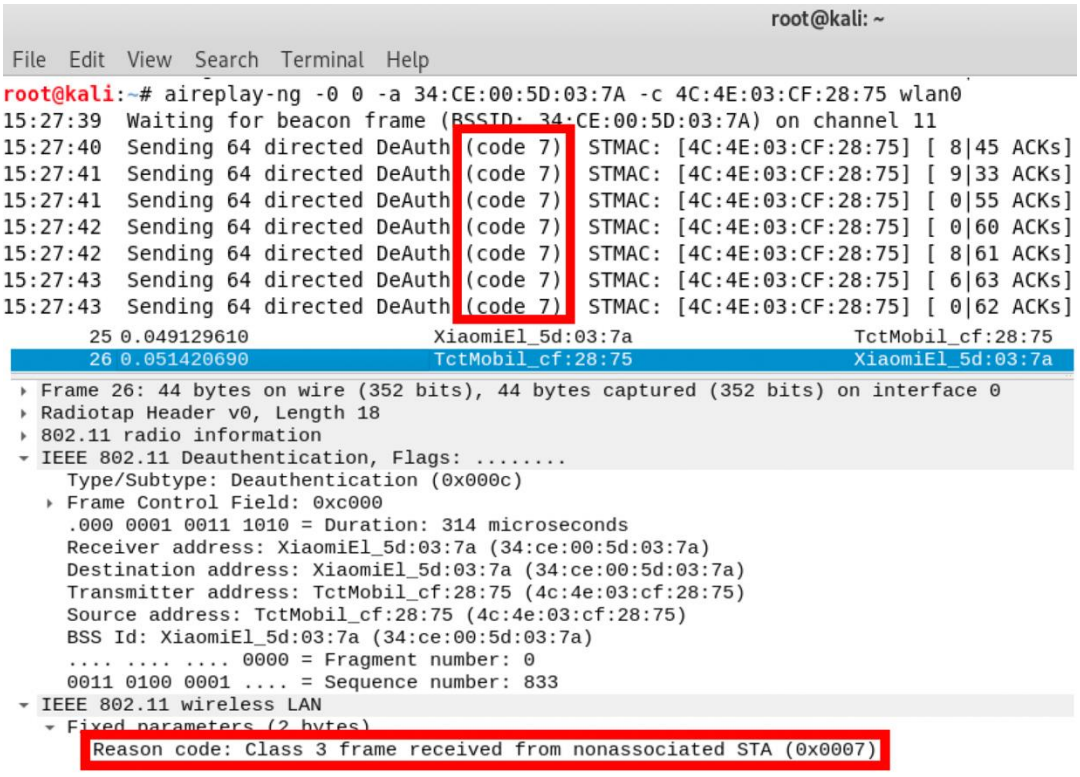

Fig.4.3 The reason code in the deauthentication frames

4.3 The level of signal strength RSSI

In case of successful deauthentication attack, the signal level of the attacker's network card is usually higher than the signal level of the legitimate AP. This is important, for example in the case of a MITM attack, when an attacker needs to use a deauthentication attack to forcibly disconnect the client from the AP and reconnect the client to a fake access point (Rogue AP) [20]. To do this, the attacker must be located closer to the AP than the legitimate client or increase the transmitter power of the network adapter that he uses to attack. Different countries have different technical regulations for Wi-Fi. While in most countries, including Ukraine, the transmitter power limit of the Wi-Fi network adapter is set to 20 dBm (100 mW), there are countries where the limit is set to 30 dBm [16]. An attacker could use that to their advantage by changing programmatically the country in which the device is expected to operate and thereby increasing the transmitter power to 30 dBm (1000 mW). The result of increasing the transmitter power of the network adapter from 18 dBm to 30 dBm is shown in Fig. 4.4.

```
root@kali:~# iwconfig
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=18 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

root@kali:~# iw reg set BZ
root@kali:~# iwconfig wlan0 txpower 30
root@kali:~# iwconfig
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=30 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Fig.4.4 Changing the transmitter power of the network adapter

After launching the deauthentication attack, the RSSI values will be different (changed). In fact, the jump values can be determined by various factors, such as the distance between the legitimate AP and the attacker's network adapter, the position of the attack detector, and the transmitter power of both devices. On the Linux operating system, the RSSI value can be obtained from the RadioTap header.
In the course of our experiments, we have recorded the average value of the signal level during the transmission of a legitimate AP and the jump of the average value of the RSSI during the deauthentication attack (Fig. 4.5).

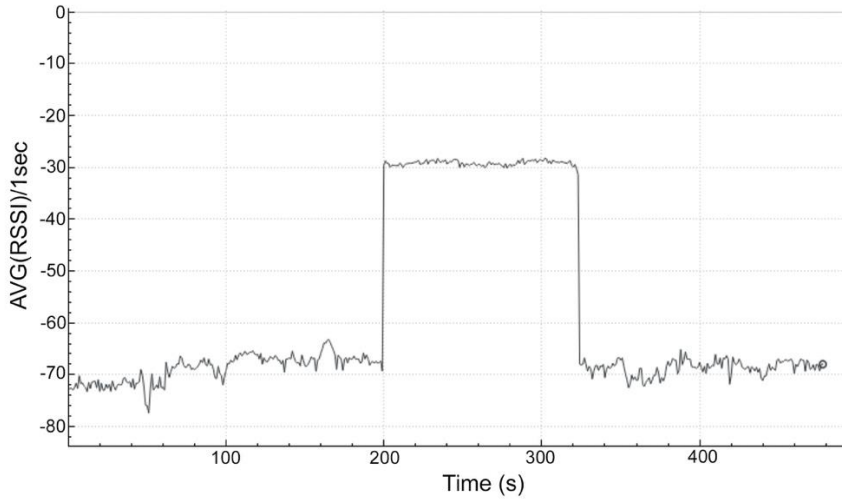

Fig.4.5 The average value of the RSSI for the legitimate AP before and during the attack

A sharp change in the RSSI value in deauthentication frames relative to other frames broadcasted by a legitimate AP may indicate an attack.

5. Literature review

Some authors propose to use the threshold number of deauthentication frames for identification of deauthentication attack [17]. When the number of deauthentication frames exceeds the threshold number, it is considered as a sign of deauthentication attack. However, there are some drawbacks to this approach. First, only one parameter is taken into account and other parameters related to the wireless network are ignored, which, in turns, leads to many false positives. Second, deauthentication frames can be sent by an attacker with variable frequency, which does not allow detecting the attack.

The two types of attacks, namely, the attack of deauthentication and the attack of the evil twin are investigated in [18]. To detect a deauthentication attack, only the reason code is taken into account. Other MAC header parameters are not considered. Because the reason code can also be included in a legitimate deauthentication frame, this detection method can increase the frequency of false positives as well.

The simplified solution to detect a deauthentication attack is proposed in [21]. The proposed algorithm uses the reason code and MAC timestamp parameters. However, the reason code can also be used by a legitimate deauthentication frame, and the deauthentication frames can be sent by an attacker at variable intervals. Therefore, we believe that those two parameters are not sufficient to reliably detect a deauthentication attack.

6. The proposed solution for detecting deauthentication attack

We offer an algorithm for detecting deauthentication attacks, which can reduce the frequency of false positives by using a combination of three parameters.

The main parameters that are considered in our algorithm to detect this attack:

1) Reason Code,

2) Timestamp,

3) Received Signal Strength Indicator (RSSI).

We propose to use a DDA (Detector of Deauthentication Attack), which scans the data of wireless traffic, analyzes them and issues a warning about a possible deauthentication attack (Fig. 6.1).

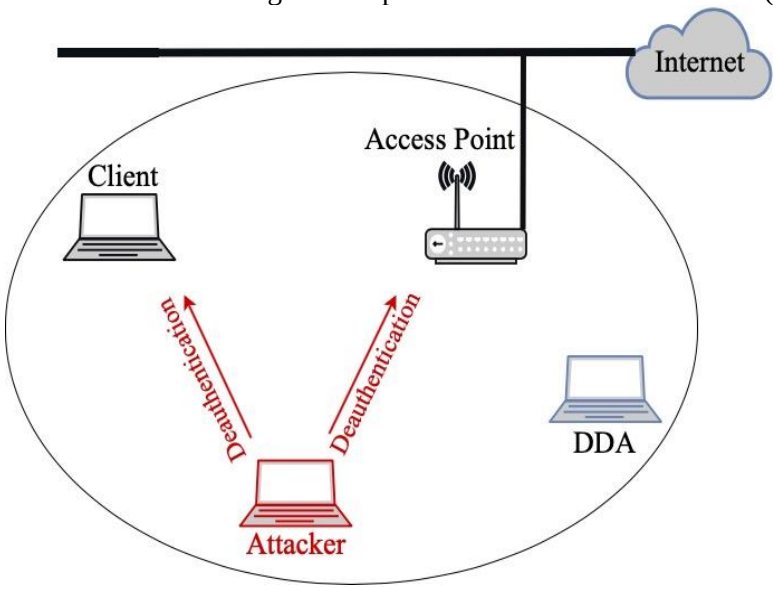

Fig.6.1 Scheme for detecting deauthentication attacks

Fig. 6.2 shows the algorithm for detecting a deauthentication attack. The DDA is started by switching the network interface to monitoring mode and switching to the appropriate AP channel. In this mode, the hardware interface is not connected to any network and is used for passive sniffing. The interface receives all packets in its listening channel for further analysis of AP frames and its associated client. The DDA analyzes the packets by extracting deauthentication frames (Type 00, Subtype 1100) from the total stream and analyzing their number per unit of time. If the value exceeds the set threshold, the DDA will issue an attack warning.

If the frequency of deauthentication frames does not exceed the set threshold, the DDA checks the reason code of the next deauthentication frame. In case the reason code is 7, the algorithm proceeds to checking the RSSI level of this frame so the final decision can be made.

After launching the deauthentication attack, DDA receives deauthentication frames with the modified RSSI values from the attacker. When $\triangle = |\overline{RSSI} - RSSI^{deauth}|$ the deviation of the RSSI value of the received deauthentication frame ($RSSI^{deauth}$) from the average RSSI values of the legitimate AP frames ($\overline{RSSI}$) exceeds the threshold value, the DDA issues an attack warning. Otherwise, the DDA monitoring node continues to monitor and analyze the received frames.

Monitoring the average values of RSSI frames from the legitimate AP is performed by means of a sliding window algorithm. The value of the RSSI level jump can be determined by various parameters, such as the distance between the legitimate AP and the attacker, the position of the monitoring node, as well as the power of the AP and the attacker's transmitters. In Fig. 4.5, the deviation of the mean RSSI value can reach 10 dBm. We propose to set the value of the attack threshold to 10 dBm. Otherwise, when the RSSI frame value deauthentication is less than 10 dBm, the DDA will assume that everything is fine. It should be noted that the 10 dBm threshold is set for the average value instead of not-averaged RSSI values, as it can often fluctuate by more than 10 dBm.

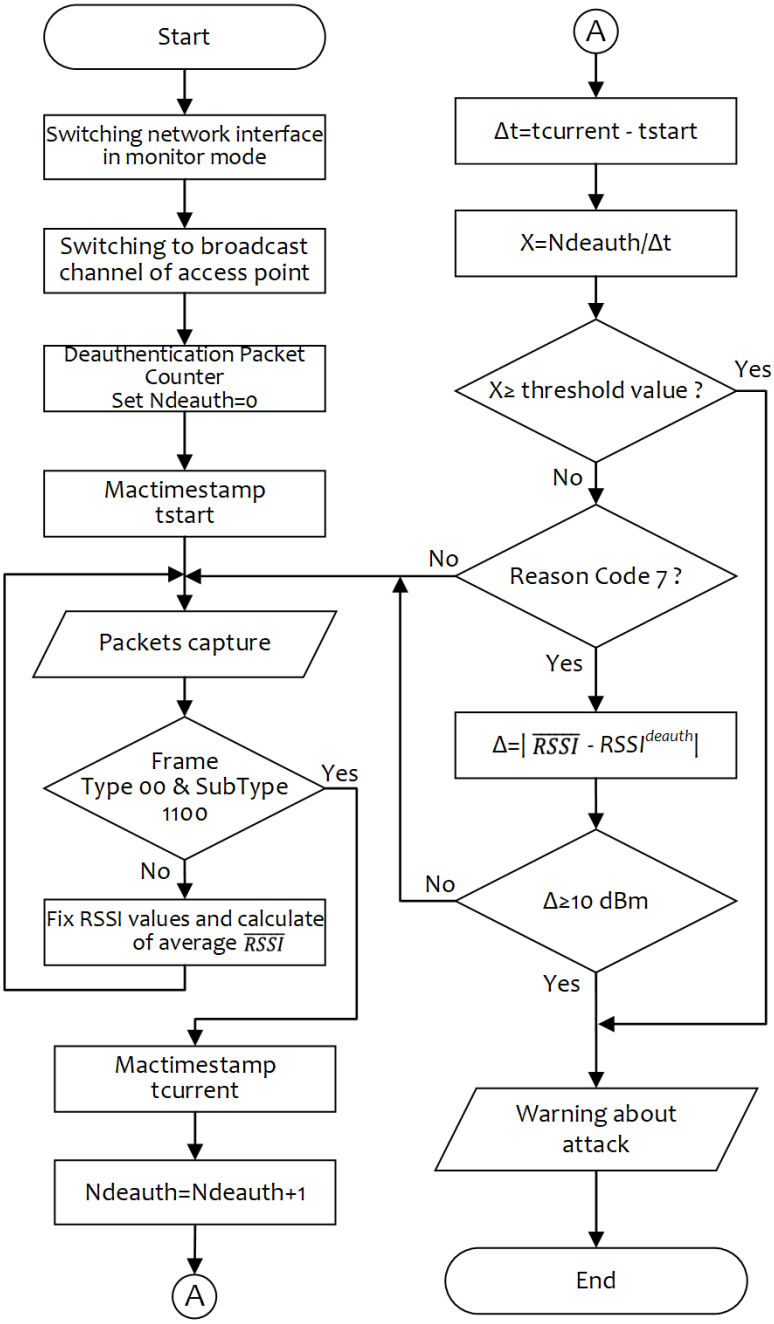

Fig.6.2 Block diagram of the algorithm for detecting deauthentication attacks

7. Conclusions

Our research and practical experiments have shown that due to the exchange of unencrypted management frames, wireless LANs are prone to DoS attacks, namely deauthentication attacks, which can completely disconnect a legitimate client from the network. Therefore, there is a need for an effective, easy and automated method of detecting attacks of deauthentication.

We propose to use the DDA, which scans and analyzes the wireless traffic data, and issues warnings in case of a possible attack. The DDA is based on a new algorithm for detecting deauthentication attacks, which uses a combination of three parameters reducing the frequency of false positives. The presented methodology is easy to implement, does not require system training, and can be used both in open and encrypted networks.

The deauthentication attack has been performed for one legitimate client in this research. Further this technique can be modified for several legitimate wireless network users. Future improvements can also increase the capabilities of the system. Due to the fact that the DDA algorithm is based on network traffic anomalies, it will be able to counteract some other threats, such as rogue access point for example.

REFERENCES

1. M. Waliullah and D. Gan, "Wireless LAN Security Threats & Vulnerabilities", *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 1, pp. 176-183, 2014 https://doi.org/10.14569/ijacsa.2014.050125
2. C. Kolias, G. Kambourakis, A. Stavrou and S. Gritzalis, "Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset", *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184-208, 2016 https://doi.org/10.1109/comst.2015.2402161
3. M. Chan Aung and K. Thant, "Detection and mitigation of wireless link layer attacks", *2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*, pp. 173-178, 2017 https://doi.org/10.1109/sera.2017.7965725
4. H. A. Noman, S. M. Abdullah, and H. I. Mohammed, "An automated approach to detect deauthentication and disassociation dos attacks on wireless 802.11 networks", *International Journal of Computer Science Issues (IJCSI)*, vol. 12, no. 4, pp. 107-112, 2015 https://www.ijcsi.org/papers/IJCSI-12-4-107-112.pdf
5. Deep Joshi, Dr. Ved Vyas Dwivedi, K.M.Pattani "De-Authentication attack on wireless network 802.11i using Kali Linux", *International Research Journal of Engineering and Technology (IRJET)*, Volume, 04 Issue, pp. 1666-1669, 2017 https://www.irjet.net/archives/V4/i1/IRJET-V4I1331.pdf
6. Korolkov R.Y. and Kutsak S.V "The features of a deauthentication attack implementation in networks 802.11", *Ukrainian Information Security Research Journal*, vol. 21, no. 3, pp. 175-181, 2019 https://doi.org/10.18372/2410-7840.21.13953 [in Ukrainian]
7. R. Cheema, D. Bansal and S. Sofat, "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks", *International Journal of Computer Applications*, vol. 23, no. 7, pp. 7-15, 2011 https://doi.org/10.5120/2901-3801
8. J. Milliken, V. Selis, K. Yap and A. Marshall, "Impact of Metric Selection on Wireless DeAuthentication DoS Attack Performance", *IEEE Wireless Communications Letters*, vol. 2, no. 5, pp. 571-574, 2013 https://doi.org/10.1109/wcl.2013.072513.130428
9. C. Kohlios and T. Hayajneh, "A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3", *Electronics*, vol. 7, no. 11, p. 284, 2018. https://doi.org/10.3390/electronics7110284
10. Mofreh Salem, Amany Sarha, Mostafa Abu-Bakr "A DOS Attack Intrusion Detection and Inhibition Technique for Wireless Computer Networks" ICGST- CNIR, Volume (7), Issue (I), pp. 17-24, 2007 http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.469.5991
11. IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), C1–1184, 2007 https://standards.ieee.org/standard/802_11-2007.html
12. Masiukiewicz Antoni, Tarykin Viktor, Podvornyi Vova, "Tools for Wi-Fi Network Security Analysis", *Vistula Scientific Quarterly*, 3(49), pp. 114-134, 2016 http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-60891997-7f20-4acc-bda8-de4e8b4a3dac/c/KNUV_3_49_2016.114-134.pdf

13. John Bellardo and Stefan Savage “Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions”, *Published in 12th USENIX Security Symposium Washington*, D.C., USA, pp. 15-27, 2003 https://cseweb.ucsd.edu/~savage/papers/UsenixSec03.pdf
14. M. Agarwal, S. Biswas and S. Nandi, "Detection of De-authentication Denial of Service attack in 802.11 networks", *2013 Annual IEEE India Conference (INDICON)*, pp. 1-6, 2013 https://doi.org/10.1109/indcon.2013.6726015
15. Deauthentication reason code table. [Online]. – Available: https://www.cisco.com/assets/sol/sb/WAP371_Emulators/WAP371_Emulator_v1-0-1-5/help/Apx_ReasonCodes2.html [Accessed: March 30, 2021].
16. How to increase wifi adapter power [Online]. – Available: https://www.kalitut.com/2019/04/how-to-increase-wifi-txpower.html [Accessed: March 30, 2021].
17. TJ OConnor “Detecting and responding to data link layer attacks”, SANS Institute InfoSec Reading Room, October 13, 2010 https://www.sans.org/reading-room/whitepapers/intrusion/paper/33513
18. Z. Afzal, J. Rossebo, B. Talha and M. Chowdhury, "A Wireless Intrusion Detection System for 802.11 networks", *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 828-834, 2016 https://doi.org/10.1109/wispnet.2016.7566249
19. A. Arora, “Preventing wireless deauthentication attacks over 802.11 networks,” *ArXiv*, vol. abs/1901.07301, 2019 https://arxiv.org/pdf/1901.07301.pdf
20. S. Wang, J. Wang, C. Feng and Z. Pan, "Wireless Network Penetration Testing and Security Auditing", *ITM Web of Conferences*, vol. 7, p. 03001, 2016 https://doi.org/10.1051/itmconf/20160703001
21. Rajinder Singh and Satish Kumar “A light weight solution for detecting de-authentication attack”, *International Journal of Network Security & Its Applications (IJNSA)* vol. 11, no.1, pp. 15-26, 2019 https://aircconline.com/ijnsa/V11N1/11119ijnsa02.pdf

ЛІТЕРАТУРА

1. M. Waliullah and D. Gan, "Wireless LAN Security Threats & Vulnerabilities", *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 1, pp. 176-183, 2014 https://doi.org/10.14569/ijacsa.2014.050125
2. C. Kolias, G. Kambourakis, A. Stavrou and S. Gritzalis, "Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset", *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184-208, 2016 https://doi.org/10.1109/comst.2015.2402161
3. M. Chan Aung and K. Thant, "Detection and mitigation of wireless link layer attacks", *2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*, pp. 173-178, 2017 https://doi.org/10.1109/sera.2017.7965725
4. H. A. Noman, S. M. Abdullah, and H. I. Mohammed, "An automated approach to detect deauthentication and disassociation dos attacks on wireless 802.11 networks", *International Journal of Computer Science Issues (IJCSI)*, vol. 12, no. 4, pp. 107-112, 2015 https://www.ijcsi.org/papers/IJCSI-12-4-107-112.pdf
5. Deep Joshi, Dr. Ved Vyas Dwivedi, K.M.Pattani “De-Authentication attack on wireless network 802.11i using Kali Linux”, *International Research Journal of Engineering and Technology (IRJET)*, Volume, 04 Issue, pp. 1666-1669, 2017 https://www.irjet.net/archives/V4/i1/IRJET-V4I1331.pdf
6. Корольков Р.Ю., Куцак С.В. Особливості реалізація атаки деавтентифікації в мережах стандарту 802.11. *Захист інформації,* 21(3), 175-181, 2019 https://doi.org/10.18372/2410-7840.21.13953
7. R. Cheema, D. Bansal and S. Sofat, "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks", *International Journal of Computer Applications*, vol. 23, no. 7, pp. 7-15, 2011 https://doi.org/10.5120/2901-3801
8. J. Milliken, V. Selis, K. Yap and A. Marshall, "Impact of Metric Selection on Wireless DeAuthentication DoS Attack Performance", *IEEE Wireless Communications Letters*, vol. 2, no. 5, pp. 571-574, 2013 https://doi.org/10.1109/wcl.2013.072513.130428
9. C. Kohlios and T. Hayajneh, "A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3", *Electronics*, vol. 7, no. 11, p. 284, 2018. https://doi.org/10.3390/electronics7110284

10. Mofreh Salem, Amany Sarha, Mostafa Abu-Bakr “A DOS Attack Intrusion Detection and Inhibition Technique for Wireless Computer Networks” ICGST- CNIR, Volume (7), Issue (I), pp. 17-24, 2007 http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.469.5991
11. IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), C1–1184, 2007 https://standards.ieee.org/standard/802_11-2007.html
12. Masiukiewicz Antoni, Tarykin Viktor, Podvornyi Vova, “Tools for Wi-Fi Network Security Analysis”, *Vistula Scientific Quarterly*, 3(49), pp. 114-134, 2016 http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-60891997-7f20-4acc-bda8-de4e8b4a3dac/c/KNUV_3_49_2016.114-134.pdf
13. John Bellardo and Stefan Savage “Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions”, *Published in 12th USENIX Security Symposium Washington*, D.C., USA, pp. 15-27, 2003 https://cseweb.ucsd.edu/~savage/papers/UsenixSec03.pdf
14. M. Agarwal, S. Biswas and S. Nandi, "Detection of De-authentication Denial of Service attack in 802.11 networks", *2013 Annual IEEE India Conference (INDICON)*, pp. 1-6, 2013 https://doi.org/10.1109/indcon.2013.6726015
15. Deauthentication reason code table. [Online]. – Available: https://www.cisco.com/assets/sol/sb/WAP371_Emulators/WAP371_Emulator_v1-0-1-5/help/Apx_ReasonCodes2.html [Accessed: March 30, 2021].
16. How to increase wifi adapter power [Online]. – Available: https://www.kalitut.com/2019/04/how-to-increase-wifi-txpower.html [Accessed: March 30, 2021].
17. TJ OConnor “Detecting and responding to data link layer attacks”, SANS Institute InfoSec Reading Room, October 13, 2010 https://www.sans.org/reading-room/whitepapers/intrusion/paper/33513
18. Z. Afzal, J. Rossebo, B. Talha and M. Chowdhury, "A Wireless Intrusion Detection System for 802.11 networks", *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 828-834, 2016 https://doi.org/10.1109/wispnet.2016.7566249
19. A. Arora, “Preventing wireless deauthentication attacks over 802.11 networks,” *ArXiv*, vol. abs/1901.07301, 2019 https://arxiv.org/pdf/1901.07301.pdf
20. S. Wang, J. Wang, C. Feng and Z. Pan, "Wireless Network Penetration Testing and Security Auditing", *ITM Web of Conferences*, vol. 7, p. 03001, 2016 https://doi.org/10.1051/itmconf/20160703001
21. Rajinder Singh and Satish Kumar “A light weight solution for detecting de-authentication attack”, *International Journal of Network Security & Its Applications (IJNSA)* vol. 11, no.1, pp. 15-26, 2019 https://aircconline.com/ijnsa/V11N1/11119ijnsa02.pdf

Надійшла – 03.04.2021.