International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6137
***Article Received**: 22 December 2022 **Revised**: 20 January 2023 **Accepted**: 29 January 2023*

Analyzing and Detecting the De-Authentication Attack by Creating an Automated Scanner using Scapy

Mustafa Abdulkareem Salman Al-Nuaimi[1], Abdullahi Abdu Ibrahim[2]
[1]Department of Information Technologies
Altinbas University
Istanbul, Turkey
Ak_mustapha@yahoo.com
[2]Department of Electrical And Electronic Engineering
Altinbas University
Istanbul, Turkey
Abdullahi.Ibrahim@altinbas.edu.tr

Abstract— with the rapid spread of internet technologies around the world, the number of people that are using theinternet is increasing enormously in the last 10 years. with the increase in the number of people that are using the internet and the increase in the devices that depend on the internet such as computers, tablets, and mobile phones are raised the challenges of internet security against hackers who can steal sensitive information and exploits personal data. In this paper, we're focusing on the home security threads and one of its famous attacks called the De-authentication attacks. The de-authentication frame is one of the Management frames that is transmitted between the AP and the connected devices and it can be used by attackers to apply a Dos attack and deny the devices from connecting to the network. In this paper. We will analyze the normal de-authentication frame and compare it with the attacking de-authentication frames to create an automated Scanner to identify whether it's an attack, or it's a normal frame transmitted between AP and its connected devices, or vice versa.

Keywords- De-authentication Attack; Kali Linux; Scapy; Wireshark; Python.

I. INTRODUCTION

Internet networks are growing fast and gaining popularity rapidly in home and all types of business industries, wireless Lan networks become more used and more widespread than wired Lan networks because of their ease of installments, more mobility, and cost less than LAN networks, because of that, every home nowadays have a wireless Lan network and it's easy to be installed by anyone without a massive experience [1]. Small homes and the simplest networks can contain a large number of devices connected that can transfer a sensitive. Small homes and the simplest networks can contain a large number of devices connected that can transfer sensitive information that can be up for grabs for hackers to exploit this information. Hackers are considering wireless LAN networks as a good environment to breach victims' devices because wireless transmission is more exposed to attacks due to its working nature that transmits data to the clients using radio waves through the air rather than wires, this lack of physical barrier makes wireless networks vulnerable such as Denial of service, eavesdropping, and other cyber security issues [2].

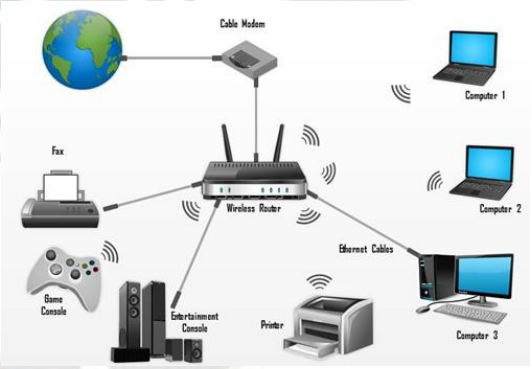

Figure 1: Simple wireless network[3]

Wireless network security is highly demanded to protect the data packets transmitted in the air, the main criteria for wireless security generally consist of five parameters: Confidentiality: which means that the data are transmitted securely without any disclosure from unauthorized users. Integrity: it means that data must be transmitted from sender to receiver without any modifications. Access Control: it means that the resources must be granted based on the authority of the users, resources such as hosting systems and applications will be limited and accessed only for specific and legitimate users. Authentication: it verifies the user's authenticity and assures that the data is transmitted from an identified user to a particular destination. Availability: Availability means that the resources are always available to be

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6137
***Article Received**: 22 December 2022 **Revised**: 20 January 2023 **Accepted**: 29 January 2023*

accessed by users, information will not be useful if it's unavailable when it is needed [4]. One of the most common attacks on wireless networks is a De-authentication attack, the De- authentication attack falls under the DOS (denial of services attack) category which attacks the Availability of the services. De- authentication Attack specifically targets the connection between the AP (Access point) and the devices connected to it [5]. The rest of the paper consists of the following sections. In II- the problem statement will discuss the introduction to the De-authentication attack and its effectiveness on the wireless networks and the tools used to apply and carry this attack have been discussed. In section III – A literature review of the De-authentication attack and proposed solutions have been discussed. In section IV- the research methodologies are discussed. Discussion of the results will be in section V and the conclusion will be in section VI.

II. Problem Statement

A de-authentication Attack is one of the famous and common attacks on wireless networks, it is considered a type of Denial of services attack which aims to break the connections between a router and its connected devices.

The De-authentication frames belong to the Management frames, management frames are transmitted frequently between the router and all its connected devices, besides other frames like Control frames and Data frames. Under normal circumstances, a device can send a de-authentication frame to the AP or router to disconnect itself from the network, or an AP can send the de-authentication frames to a specific device to disconnect it from its network. Unlike other frames, de-authentication frames are not encrypted during the transmission, so it's easy to be used from hackers to broadcast de-authentication frames to devices and AP and deny the service on them and apply the De-authentication Attack.

The common security approaches for wireless networks are based on IEE802.11 standards, but an increase in the use of wireless networks made the de-authentication attack more serious because most of the IEE802.11 protocols do not encrypt the de-authentication transmitted frames yet, only 802.11w protocol-protected the whole management frames but it's not supported in all routers or devices yet. In addition to the newest security protocol WPA3 protocol. IEEE 802.11w is a standard for wireless security that adds more protection to the management frames that are exchanged between clients and routers. We can observe that not all devices support IEEE 802.11w due to a variety of reasons such as Hardware Limitations, framework incompatibility, Lack of implementations, and interoperability issues. overall, the use of IEEE802.11w is still not very popular and it may take more time for it to become widely separated in the wireless industry.

The goal of the De-authentication attacks is not only for denying a service from a particular device or all devices, it can be used for more attacks, like brute force, brute force attacks can be used to crack Wi-Fi passwords and depends on the De-authentication attack to force the devices to be disconnected from the AP and when a device tries to reconnect, a special tool will be used to capture the information sent from the device to the AP and it contains the authentication information to be stolen.

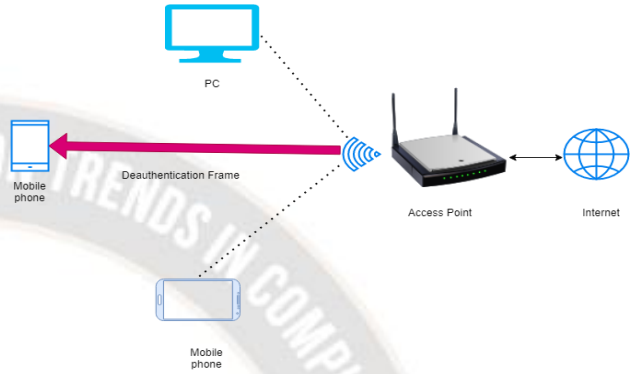

Figure 2: Normal De-authentication frame process

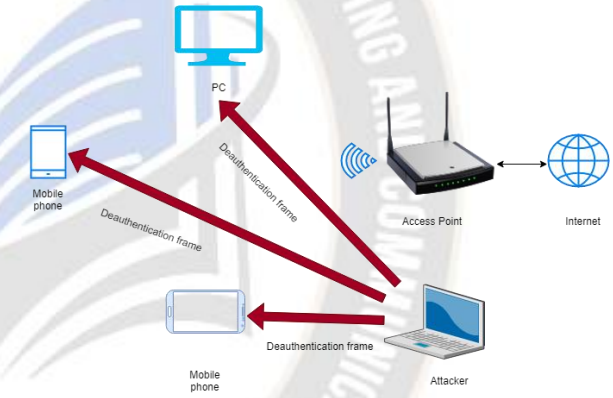

Figure 3: De-authentication attack scenario

In this paper, the attack simulation has been done with two tools**: i- Kali Linux**: is a Debian-based Linux, an open-source software aimed at advanced penetration testing and security Auditing. Kali Linux contains many tools that targeted information security tasks, such as security research, vulnerability management, and penetration testing [6]**. ii-scapy**: scapy is a python program that can manipulate packets. It's able to forge and decode packets, send them, capture them and compare between the requests and replies, and much more. Scapy can do much more tasks like scanning, tracerouting, attacks, and network discovery. Simply, you can send an invalid frame or inject your own 802.11 frames [7].

III. Literature Review

Haitham Noman, Mohd N Shahidan, and Haydar Imad Mohammed.[8] focuses on the availability factor of the wireless networks and disrupted the connection between authorized clients by sending forged packets that contain the de-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6137
***Article Received**: 22 December 2022 **Revised**: 20 January 2023 **Accepted**: 29 January 2023*

authentication frames using "IJAM" a python customizable tool, the author also discussed the ways to detect the attacks using an automated detection mechanism and it was effective in Linux environment and it doesn't run on windows due to its limitations and it depends only on the type and the subtypes of the management frames. They also claimed that the current standards need urgent patches to protect Wi-Fi networks more effectively. The Author [1] described a lightweight solution to detect the de-authentication attack by suggesting algorithm-based radio-tap header information to identify whether it's a de-authentication attack on the client or not. This algorithm uses the reason code and MAC time stamp as a parameter to reduce the positive false rates. We assume that the parameters are not accurate enough and it needs more factors to be considered. The Author in [9] suggested an algorithm to make more immune from de-authentication attacks and implemented it in real-time scenarios, the results show that the proposed technique raises the packet flow rate by 20.36% and reduces the packet loss by 95% approximately, the downtime and the recovery time are reduced slightly. In [9] research, the de-auth attack is performed against a single legitimate user. The author [5] stays around the Wi-Fi Dos attack and practical detection of it by using Scapy, the author [5] practically conducted a de-auth attack and wrote a scapy python script to detect it and depends on the time of the attack, De-auth layer and type/subtype of the De-authentication frame inside the Management frames. The results are not accurate enough because it may consider the normal de-authentication frame from AP to the client or vice versa as an attack. The author [10] aimed to know the security level of WIFI security against de-authentication attacks in the internet of things (IoT)-based devices. The author [10] did it by testing an external penetration test method that simulates a real external attack from an attacker without information about the target. The author [10] results that DE- authentication attack communication paralysis between the connected devices with several changes in data rates, frequency channels, and retry bits in management frames. The author [10] concluded that the IEEE802.11 frame management needs improvements and should analyze a solution to deal with De-authentication Attacks on Wireless networks.

Table 1: Literature Review Summary

Year	Author	Aim of study	Researcher opinion
2015	H.Noman, N Shahidan, and Haydar Mohammed	Automated detection mechanism	Depends only on the type and subtype parameters
2019	R. Singh and S. Kumar	A lightweight solution to detect the attack	Depends only on the MAC time stamp and the reason code
2020	S. Sharma and M. Mittal	Detection and prevention of de-authentication attacks in real-time scenario	The attack is performed on a single legitimate client
2020	R. Poudél	Practically detecting WIFI Deauthentication attack	Depends only on the De-auth layer and type/subtype parameters
2020	Y. Kristiyanto and E. E	Analysis of deauthentication attack on IEEE 802.11 connectivity based on IOT technology using external penetration test	De-auth attacks communication paralysis between the connected devices.

IV. Research Methodologies

A. Working Environment: in this paper, we have an AP which it will be attacked and also defended, we used a Raspberry Pi 4B which is installed as a home Router with an OpenWrt kit. Raspberry pi is a very cheap and small computer that runs on Linux, and it also has general-purpose input and output pins that allow us to control electronic and electrical components and IoT [11]. In addition to that, Raspberry pi can be programmed to work as many devices as we need, like a Router or AP. in our experiments, we used the OpenWrt kit to transform our Raspberry pi into a router. OpenWrt is a Linux operating system targeting embedded devices. Instead of creating a static framework. OpenWrt provides a flexible filesystem and package management [12]. Next, we have an attacker, which will attack the wireless network and denial its services to the clients by sending neuromas number of de-authentication frames to the router. The attacker used Kali Linux which is a Linux operation system used generally on penetration tests, attacks, and other cyber security purposes. As an attacker, we applied two types of De-authentication attacks, the first attack was applied using a python library called Scapy to forge and send customizable packets with our De-authentication frames to disconnect the router from its devices. The second type of attack was applied using Aireplay-ng, a Linux tool that is used to inject frames, its function is to create a flow of traffic for later use generally with Aircrack-ng which is used to crack wi-fi passwords [13]. It's noteworthy that the first type of attack was much more flexible than the second one due to its limited properties, but the second type is a much more famous tool for hackers and is widely used to attack home wireless networks, so we can consider it as standard due to its popularity and we can compare it with our customizable attack to analyze the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6137
***Article Received**: 22 December 2022 **Revised**: 20 January 2023 **Accepted**: 29 January 2023*

similarity and differences in victim's point of view. Next, we used Wireshark, it's a network protocol analyzer, it lets you see what's happening to your network in deep detail. We will use Wireshark to analyze the incoming de-authentication packets that came from the real clients and attackers and analyze the results and the difference between these packets. Finally, we must use an external wireless Antenna that contains a Monitor mode to have the ability to scan and sniff the networks, not all wireless adaptors have this mode so we must use a special type of wireless adaptor. We used an ALFA adaptor with model AWUS036H, it worked well and captured all packets between the routers and their clients, but its main problem is that it can only capture 2.5ghz bands because it's an old module so we will focus only on 2.5ghz. The experiment environment is simplified and shown in fig4.

B. performing an Attack on the raspberry pi router: as we said earlier in the working environment, we will apply two types of attacks. For the first attack, we will use a scapy python code to perform de-authentication traffic that will disable the connection between the router and its connected devices as follow:

1- convert the wireless adapter from the Managed mode to the Monitored Mode.
2- importing scapy library
3- setting the interface of the monitor adapter (ALFA)
4- setting the BSSID of the router
5- specifying the BSSID of the victim, we set all the connected devices as targeted devices.
6- forge the customizable de-authentication packet to send.
7- send the forged packet to the target.

In this code, we sent 1000 De-authentication frames to the devices and disable them from the router with 0.1ms for each frame. The connection will be back to normal condition when the 1000 packets are consumed. It is noteworthy that we can send any number of packets and we can specify our reason code for it.

Figure 4: Working Environment

The second attack type will be using the Aireplay-ng package to attack using a de-authentication frame to disable the connection:

1- convert the wireless adapter from managed mode to monitor mode using airmon-ng:
Sudo airmon-ng start wlan0.
2- searching for the available Wi-Fi networks around and coverable to the wireless adapter using Airodump-ng:
Sudo airodump-ng wlan0
3- after the Wi-Fi networks shown with their Bssid, SSID, and channels, we will use the airodump-ng with Bssid and channel values of the targeted router to start to listen to the incoming packets and save it in a .cap file in the computer which contains all the captured packets and frames:
Sudo airodump-ng w- hack1 –c [channel] -–bssid <Bssid> wlan0
4- finally we can use the Aireplay-ng tool to attack the target with a De-authentication flow of packets to disable its services and disconnect its connected devices:
Sudo Aireplay-ng –deauth 0 -a <Bssid> wlan0
This attack will apply a de-auth attack with infinite times until the attacker stops the attack and the reason code for this attack will be fixed on 7. This attack forces the devices to be disconnected and when one of these devices tries to reconnect, the Airodump-ng script will capture the packets that contain the authentication information to be cracked using Aircrack-ng.

V. Results and Discussion

Our model was designed to detect De-authentication DOS attacks more efficiently and with more accuracy can allow the owner of the network to differentiate between the legitimate de-authentication frames and attacks by considering four parameters to identify the incoming frame. 1-Counted Frames numbers: when we send the de-authentication frame from a device to AP or vice versa, it will use a few numbers of De-authentication frames to make the device disconnect from the network, the maximum number of used frames analyzed was 4 frames only per request. So, in normal states, the AP and any device don't need to send a huge number of frames to deny a device from work at the same time. Plus, the attacker obviously will attack the network with an enormous number of frames to deny devices from services and guarantee that the authentication credentials will be captured (in a password-cracking attack). It's noteworthy that the AP only needs to send De-authentication frames when the banned device tries to access the network, continuously. 2-Frame length: we noticed that the Frame Length from the real AP or Devices is fixed to 44 bytes (352 bits) on the interface. But the Frame length from an attacker is not fixed, between 39 bytes and 34 bytes as experienced against 10 sample frames as shown:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6137
***Article Received**: 22 December 2022 **Revised**: 20 January 2023 **Accepted**: 29 January 2023*

Table 2: Normal De-authentication frame analysis

Frame No.	Frame Time	Destination Mac	Source Mac	protocol	Length
1	28.5184748	de:2b:c1:16:1e:45	Tp-LinkT_d5:f6:ae	802.11	44
2	35.62766157	de:2b:c1:16:1e:45	Tp-LinkT_d5:f6:ae	802.11	44
3	40.08174233	de:2b:c1:16:1e:45	Tp-LinkT_d5:f6:ae	802.11	44
4	44.83158708	de:2b:c1:16:1e:45	Tp-LinkT_d5:f6:ae	802.11	44
5	49.92110937	de:2b:c1:16:1e:45	Tp-LinkT_d5:f6:ae	802.11	44
6	54.03850309	de:2b:c1:16:1e:45	Tp-LinkT_d5:f6:ae	802.11	44
7	57.20952704	de:2b:c1:16:1e:45	Tp-LinkT_d5:f6:ae	802.11	44
8	60.11413229	de:2b:c1:16:1e:45	Tp-LinkT_d5:f6:ae	802.11	44
9	63.61014951	de:2b:c1:16:1e:45	Tp-LinkT_d5:f6:ae	802.11	44
10	66.73317737	de:2b:c1:16:1e:45	Tp-LinkT_d5:f6:ae	802.11	44

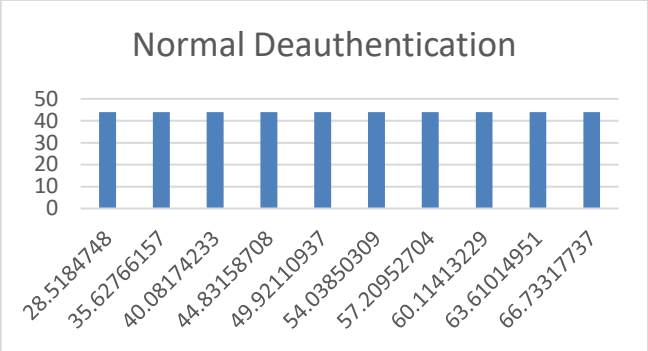

Figure 5: Normal frames length (x axis = frame time, y axis = frame length)

Table 3: De-authentication attack frames analysis

Frame No.	Frame Time	Victim AP Mac	Victim destination	protocol	length
1	79.31394887	Raspberr_a2:d6:db	Broadcast	802.11	34
2	79.32593319	Raspberr_a2:d6:db	Broadcast	802.11	39
3	79.41494565	Raspberr_a2:d6:db	Broadcast	802.11	34
4	79.42611085	Raspberr_a2:d6:db	Broadcast	802.11	39
5	79.51691355	Raspberr_a2:d6:db	Broadcast	802.11	34
6	79.52853225	Raspberr_a2:d6:db	Broadcast	802.11	39
7	79.61857859	Raspberr_a2:d6:db	Broadcast	802.11	34
8	79.62800652	Raspberr_a2:d6:db	Broadcast	802.11	39
9	79.71955016	Raspberr_a2:d6:db	Broadcast	802.11	34
10	79.73069539	Raspberr_a2:d6:db	Broadcast	802.11	39

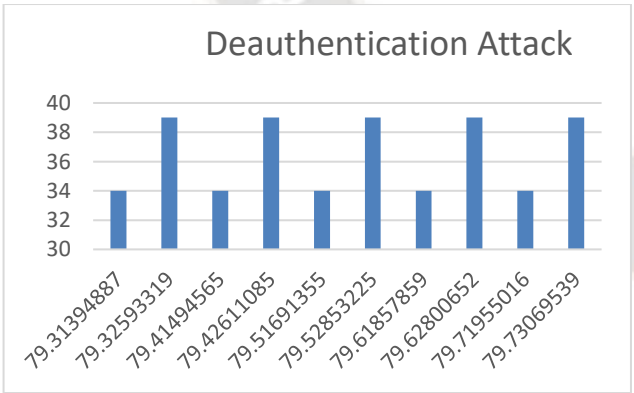

Figure 6: Attack frame length: (x axis=frames time, y-axis = frame length)

3- Frames time differences: as we can see in fig7, the time difference between the Normal frames received is much bigger than the time difference between the attack frames because the normal frames are applied when needed, but the attack frames are applied continuously:

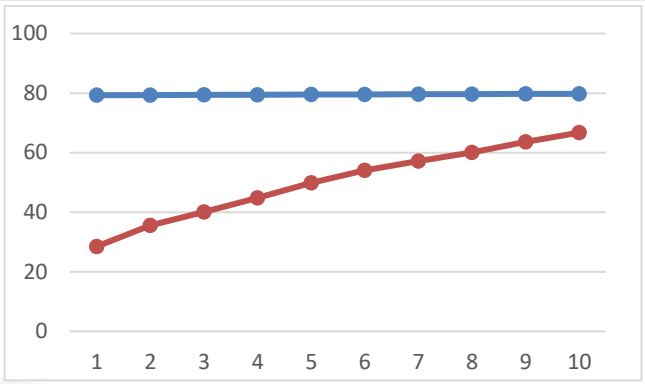

Figure 7: Time Difference between Normal frames and attack frames (Blue line: Attack frames, orange line: Normal frames, x-axis = frame number, y-axis: frame time)

4- Reason Code: Reason code is 2 bytes of fixed parameters that specify the actual reason for the De-authentication request or send, the attacking software (Aireplay-ng) is always using the reason code 7, Reason code: Class 3 frame received from no associated STA (0x0007), but with our customizable attack python code, we can specify our reason code. With the normal de-authentication frames, the reason code will vary between 0 to24 so it can be a parameter to be considered as shown in Table 4:

Table 4: Normal and Attack frames Reason codes

Frame Number	Normal Frame Reason Code	Attack Frame Reason Code
1	0x003	0x0007
2	0x006	0x0007
3	0x003	0x0007
4	0x003	0x0007
5	0x006	0x0007
6	0x003	0x0007
7	0x003	0x0007
8	0x006	0x0007
9	0x007	0x0007
10	0x003	0x0007

With these four parameters, we built our model to create the scanner that will detect whether the incoming frames are normal or it's an attack. The flowchart of our model will be shown in fig8:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6137
***Article Received**: 22 December 2022 **Revised**: 20 January 2023 **Accepted**: 29 January 2023*

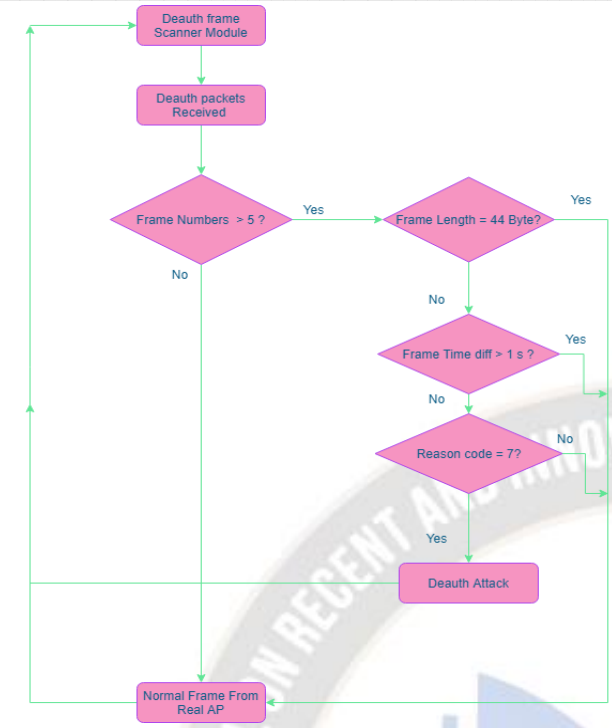

Figure 8: De-authentication attack detector model

Our proposed model is created by python programming language with Scapy library, and we used an ALFA wireless adapter to monitor and capture the incoming frames:

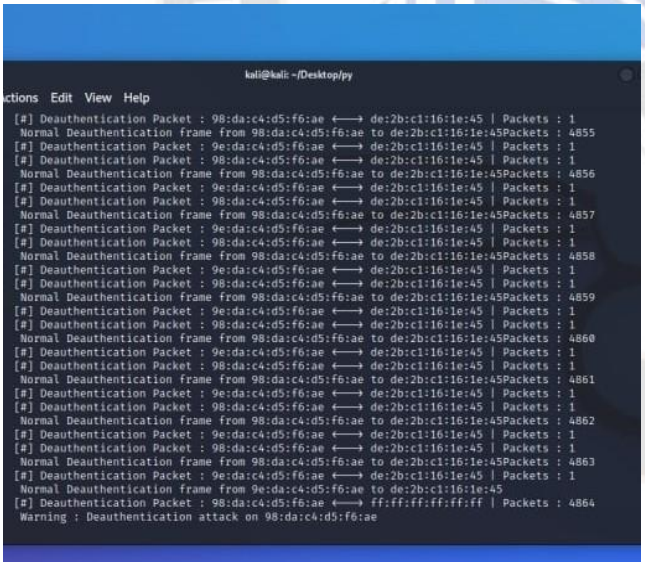

Figure 9:De-Authentication Scanner

Comparison with the other methods: Author [1] suggested a lightweight solution to detect the de-authentication attack by suggesting algorithm-based radio-tap header information to identify whether it's a de-authentication attack on the client or not. This algorithm uses the reason code and MAC time stamp as a parameter to reduce the positive false rates, but our method used more parameters (Frame number, Length, Time differences, and reason code) and it will give more accurate results. Author [9] experiment was used on a single client, while our experiment used 10 clients. Author [5] and Author [8] suggested a detection solution with only type and subtype layers as a parameter while our model is more accurate because it depends on more specific parameters. Author [10] was focusing on the IoT device's security and the effect of a De-authentication attack on it, but our method does not follow the approach of IoT devices.

VI. Conclusion

In this paper, we described a simple and basic solution to detect the De-authentication attack and make more accuracy to differentiate between the De-authentication attack from hackers and the normal De-authentication frames transmitted between the AP or a router and its connected clients, its written by python and uses Kali Linux environment, it cannot be used on windows unfortunately because it needs a monitor mode Wi-Fi adaptor and this setting is unavailable in windows features. Our solution used four parameters to be considered (Frame numbers, frame length, frame time differences, and reason code) to reduce the false positive rates and it can be useful for future research.

Acknowledgment

I would like to express my sincere gratitude to all those who have contributed to the successful completion of this research paper. Firstly, I would like to thank my supervisor Asst. Prof. Dr. Abdullahi Abdu IBRAHIM for his constant guidance, invaluable support, and insightful feedback throughout the research process. His expertise and advice have been instrumental in shaping the direction of this study.

Finally, I would like to thank my family for their support, patience, and valuable suggestions. Their constant encouragement and motivation have helped me to overcome various challenges and obstacles encountered during my study.

References

[1] R. Singh and S. Kumar, "A light weight solution for detecting de-authentication attack," International Journal of Network Security & Its Applications, vol. 11, no. 01, pp. 15–26, 2019.

[2] "Securing your wireless network," Security issues in wireless networks. [Online]. Available: https://www.nibusinessinfo.co.uk/content/security-issues-wireless-networks. [Accessed: 06-Nov-2022].

[3] "0914 home wireless network diagram networking wireless PPT slide," SlideTeam. [Online]. Available: https://www.slideteam.net/0914-home-wireless-network-diagram-networking-wireless-ppt-slide.html. [Accessed: 06-Nov-2022].

[4] "Cryptography and network security principles," GeeksforGeeks, 05-Jun-2022. [Online]. Available:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6137
***Article Received**: 22 December 2022 **Revised**: 20 January 2023 **Accepted**: 29 January 2023*

https://www.geeksforgeeks.org/cryptography-and-network-security-principles/. [Accessed: 06-Nov-2022].

[5] R. Poudél, "Practically detecting WIFI Deauthentication attack, 802.11 Deauth ...," Researchgate. [Online]. Available: https://www.researchgate.net/publication/343472668_Practically_Detecting_WiFi_Deauthentication_Attack_80211_Deauth_Packets_using_Python_and_Scapy. [Accessed: 07-Nov-2022].

[6] "What is Kali Linux?: Kali linux documentation," Kali Linux, 09-Sep-2022. [Online]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Accessed: 08-Nov-2022].

[7] Philippe Biondi and the Scapy community. (n.d.). Scapy. Retrieved December 7, 2022, from https://scapy.net/

[8] H. Noman, M. N. Shahidan, and H. I. Mohammed, "An automated approach to detect deauthentication and disassociation dos ...," Researchgate, Jun-2015. [Online]. Available: https://www.researchgate.net/publication/283354063_An_Automated_Approach_to_Detect_Deauthentication_and_Disassociation_Dos_Attacks_on_Wireless_80211_Networks. [Accessed: 11-Nov-2022].

[9] S. Sharma and M. Mittal, "Detection and prevention of de-authentication attack in real-time scenario," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 3324–3330, 2019.

[10] Y. Kristiyanto and E. E, "Analysis of deauthentication attack on IEEE 802.11 connectivity based on IOT technology using external penetration test," CommIT (Communication and Information Technology) Journal, vol. 14, no. 1, p. 45, 2020.

[11] "What is a Raspberry Pi?," Opensource.com. [Online]. Available: https://opensource.com/resources/raspberry-pi. [Accessed: 11-Nov-2022].

[12] R. Brown, "Welcome to the OpenWrt project," OpenWrt Wiki, 05-Sep-2022. [Online]. Available: https://openwrt.org/. [Accessed: 11-Nov-2022].

[13] "Aircrack-ng," aireplay-ng [Aircrack-ng]. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=aireplay-ng. [Accessed: 12-Nov-2022].