WiFi Deauthering System

Course Title: Micro Controller Lab

Nusrat Jahan Akhi
ID-1901040
Department of ICT
Faculty of Engineering
Program:Internet of Things
kaliakoir,Gazipur
1901040@iot.bdu.ac.bd

T. M. Mehrab Hasan
ID-1901049
Department of ICT
Faculty of Engineering
Program:Internet of Things
kaliakoir,Gazipur
1901049@iot.bdu.ac.bd

***Abstract*—The research aims to know the level of security of WiFi connectivity against deauthentication attacks on Internet of Things (IoT)-based devices. It is done through testing using an external penetration test method. The external penetration test simulates areal external attack without information about the target system and network given. The process starts from accessing the device through Internet or WiFi by the test target. At the same time, the attacker performs Denial-of-Service (DOS) attacks on WiFi. The attacker uses Arduino ESP8266 Endemic WiFi with Arduino programming. To record WiFi activities, the researchers use Comm View for WiFi V. 7.0, and the target is Internet Protocol (IP)camera device. The result shows that the communication of the test target with the gateway is lost, but the Media Access Control (MAC) of the test target is still registered at the gateway. Deauthentication attacks cause communication paralysis, and several changes occur, such as an increase in data rate, and change in frequency channel, Distribution System (D'S) status, retry bits in frame management, and the sequence number.**

***Index Terms*—NodeMCU ESP8266, USB Cable, Arduino, WiFi Device.**

I. Introduction

A Wi-Fi is a trade mark term used for IEEE 802.11 set of LAN protocols that implements wireless local area network (WLAN) in various frequencies. The IEEE 802 protocol specifies physical layer (PHY) and media access control layer (MAC) protocols to implement WLAN.

Radio-Frequency Identification (RFID), Wireless Sensor Networks (WSN) such as WiFi [2]. WiFi systems are widely used in homes, factories, offices, and many public places as Internet access points, and the starting point for many Internet gateways that will be needed to complete IoT coverage. WiFi is the obvious choice for IoT connectivity because its coverage in buildings is almost everywhere now. However, it is not always the right choice in the category of reliability and security. The IEEE 802.11 protocol is still classified as vulnerable as these security gaps affect the work of IoT technology [3]

The Wi-Fi works on the RF (radio frequency) technology since there is no physical connection between the sender and the receiver. It functions when a frequency within the electromagnetic spectrum associates with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space.

The wireless connection has an end point named as the Access point (AP).The key job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wireless network adapters.

Wi-Fi is supported by many applications and devices including video game consoles, home networks, PDAs, mobile phones, major operating systems and other types of consumer electronics. Any products that are tested and approved as "Wi-Fi Certified" (a registered trademark) by the Wi-Fi Alliance are certified as inter-operable with each other, even if they are from different manufacturers. For example, a user with a Wi-Fi Certified product can use any brand of access point with any other brand of client hardware that also is also "Wi-Fi Certified". Products that pass this certification are required to carry an identifying seal on their packaging that states "Wi-Fi Certified" and indicates the radio frequency band used (2.5GHz for 802.11b, 802.11g, or 802.11n, and 5GHz for 802.11a).

A Deauther allows you to **disconnect devices from a WiFi network.** Even if you're not connected to that network. Deauthers take advantage of a **weakness in the 802.11 protocol** which allows the sending of deauthentication frames by unauthorised devices.

Deauthers come with other features such as:
(a) Beacon Spamming (spamming WiFi network names)
(b) Probe Spamming (capturing the management frame)

II. Manual System

IEEE 802.11 networks or WiFi connectivity use radio waves to send information wirelessly over a LAN. Its reach can be extended by expanding Wi-Fi coverage. The IoT model that appears "smart" by connecting sensors via WiFi to cloud services and managing them and data traf[U+FB01]c. Then, this service offers a portal for analytic and smartphone-based user controls. IoT sensors must be con[U+FB01]gured to connect it to WiFi using three parameters. Those are network discovery, authentication, and device identity [4].

The fast development of the IEEE 802.11 networks has become the main target of attackers. They attack for various reasons, ranging from simple entertainment to cyber-terrorist attacks or making a pro[U+FB01]t. It is possible mainly because of wireless transmission media.It is proven to be far more vulnerable than traditional wired networks [5].

III. Automated System

The type of Denial-of-Service (DOS) attack on Wi-Fi can cause communication paralysis between connected devices. The process of this attack occurs in the authentication. It is done by sending broadcast addresses and changing broadcast addresses on targets attacked. In this case, the devices are connected through WiFi. This attack is called deauthentication. The absence of secure authentication also uncovers the devices to many other security threats that may lead to malicious attacks such as DOS attacks [6].

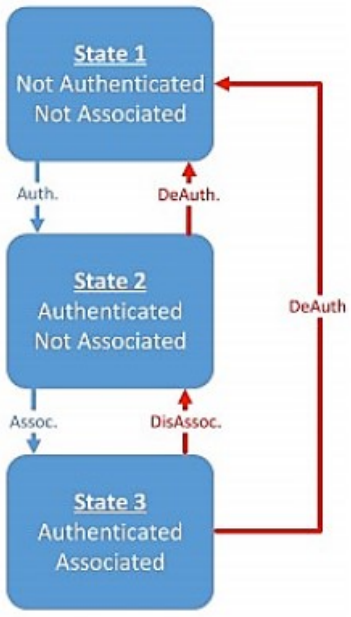

Fig. 1. Authentication State Machine.[8]

DOS attacks on WiFi are mainly caused by frame management authentication, association, deauthentication, and forged disassociation. In general, DOS attacks on WiFi can be classi[U+FB01]ed into two categories, one of which refers to attacks the target. They are authentication blocking attacks and association [U+FB02]ooding attacks [7].

IV. Background

Deauthentication is the most common form of the IEEE 802.11 DoS protocol. Previously, authentication requests a connection. After successful authentication consisting of two acknowledged authentication frames, the client station will request the association. Association response frames follow frame request association. Each frame is also recognized. The next step depends on the type of security used on WiFi and determines how intrusive the deauthentication attack is. Then, all Layer 2 management frames are broadcasted in plain text so that the closest device can find the network and request a connection.Many security problems arise from this lack of protection. If an attacker captures this plain text management frame, she/he can fake a package that seems to come from the victim [8]. This process can be seen in **Fig. 1**.

All packets transmitted over IEEE 802.11 network have homogeneous headers. Those help the attacker to guess the first eight bytes of the headers [9]. The IEEE 802.11 encryption schemes do not encrypt the management and control frames, making them vulnerable to sponge attacks. The deauthentication frame is a management frame. It is sent in plain-text which guarantees faster processing and low computation for the Access Point (AP). However, spoofing plain-text frames are trivial. As deauthentication frames are sent in plain-text, AP cannot verify the authenticity of these frames. As a result, the AP processes spoofed the deauthentication frame(s) [10].

V. Overview

Based on the background, the research aims to know the level of security of IEEE 802.11 or WiFi connectivity against deauthentication attacks on IoT based devices. It is done through testing using an external penetration test method. The results are expected to provide information for mitigating deauthentication attacks using the external penetration test.

VI. Objective of The Project

Deauthers main purpose is to demonstrate a flaw in the Wi-Fi protocol. Using this deauther you can select a certain Wi-Fi network, then with a click of a button all devices within range connected to that network will be disconnected. As long as the attack is still running, no devices within range will be able to reconnect to that network.

The deauther has the feature that will spam a custom list of Wi-Fi network names within range. You can't actually connect to these networks, but they will confuse anyone

looking for a Wi-Fi network.

The major significance of a Wi-Fi Deauther lies in the difference between Wi-Fi jammers and Wi-Fi deauthers. Sometimes both the terminologies can be confused into similar but they are diverse.

The Wi-Fi jammers basically throw out a loud noise on all Wi-Fi channels making the frequencies unusable in a given distance from the jammer. Jammers stand the disadvantage of being expensive as well as being illegal. They are hard to find unless build one by own self.

Wi-Fi deauthentication works differently compares to jammers. Wi-Fi sends encrypted data but the management frames are unencrypted. Therefore malicious parties can send deauthentication commands which boot users off an access point. [2]

VII. Literature Survey

A number of experiments have been previously done for deauthentication. Among them the best experiment was the penetration test. Penetration test is actually the planning phase where the external penetration has been carried out. In this test, the test is divided in to two terms,

- The Test Target
- The Attacker

The penetration test is a method for actively evaluating and assessing network security or information systems. It is done by simulating attacks from the attacker's perspective. It is used by an attacker to gain unauthorized access to the organization's network system and take unwanted actions [12]. The external penetration test is also known as the black box penetration test. It tries to simulate a real external attack without information about the target system and network given to the examiner. The phases of a penetration test can be seen in **Fig. 2**.

With information on penetration test phase and penetration test tools, it aims to simulate a deauthentication attack on a Wi-Fi IP that can be accessed via the Internet. In this case, it is called a target and gateway. The test is carried out on WiFi connectivity using attacker tools. During the test period, the data are recorded by using network analyzer and packet sniffing software.

A. *Penetration Test Phase*

First, in the planning phase, it needs a clear definition and scope to what extent that external penetration test is carried out. Moreover, it requires preparations in the form of information and actions to be taken during the external penetration test. The plan must also be made for test scenarios. The data are collected and used as an information, and the scenario is made in this phase. With the scenario created, it is expected that the testing is not outside the problem boundary.

Second, it is discovery. In this phase, it aims to find information related to test targets. This phase is the beginning of the recording stage as the data collected is used as material for testing at the attack stage. In this case, it is done by sending external fake packets into WiFi system. The process is referred to as deauthentication, which performs active and passive scans of WiFi signals in the area without entering the WiFi network.

Fig. 2. Penetration Test Phase.[11]

Third, the current attack process uses comparison parameters before being attacked and after being attacked.

Fourth, there is reporting. The last stage of the penetration test is useful as a reference point for defining preventive actions and mitigation activities to address identified vulnerabilities. The results of the test are reported into a digestible report for reading.

B. *Penetration Test Tools*

The tools used are:

1) Network analyzer and packet sniffer software: It is programmed for analyzing network performance such as Comm view.

2) Attacker tools: It is an IoT-based simulation device for deauthentication attacks using the ESP8266 module, NodeMCU tools, and Arduino programming.

3) Gateway: It is a network device that contains a transceiver and antenna for transmitting and receiving signals to and from remote clients using standard IEEE 802.11 WiFi

connectivity while also providing internet access to clients.

4) Computer: Intel Core-i5, DDRIV 8GB, 1 TB HDD, Windows 11 pro 64 Bit.

5) Target: The device used is other Wi-Fi device. It is connected to a gateway that can be accessed from the local network or the Internet over WiFi connectivity.

C. External Penetration Test

It is necessary to have a scope and definition of to what extent external penetration tests are carried out. The preparations in the form of information and actions must be done. This created scenario is to simulate a deauthentication attack on a device with IEEE 802.11 (WiFi) connectivity. The process of this scenario aims to record all activities when the attack process occurs using tools that have been prepared.

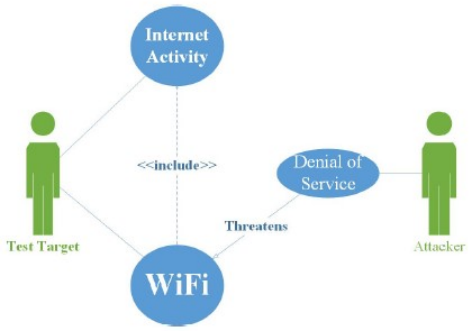

Fig. 3. UML Diagram for External Penetration Test

the actors involved are test target as victim and attacker as perpetrator. The process starts from accessing the device through Internet or WiFi by the test target. At the same time, the attacker performs DoS attack on WiFi. The scenario is done to see the DoS attack on the target so that the test targets cannot access the Internet. The initial condition is connected, while the final condition is disconnected. The carried out scenario is to understand and achieve the objectives of the external test penetration results.

UML diagram is needed to find out the process and network diagram to clarify how the scenario will be run along with penetration test tools needs. It can be seen in **Fig. 3**. For more details, the flow of attacks is in **Fig. 4**. When the test target tries to access an IoT device using WiFi, it cannot be accessed because the attacker has disconnected the WiFi connectivity. The attacker uses Arduino ESP8266 NodeMCU WiFi with Lua programming. The program script will execute the deauthentication attack method on the target. The device works by connecting the ESP8266 NodeMCU WiFi device via a gadget (notebook, mobile, and others), and calling the device's web server application [13].

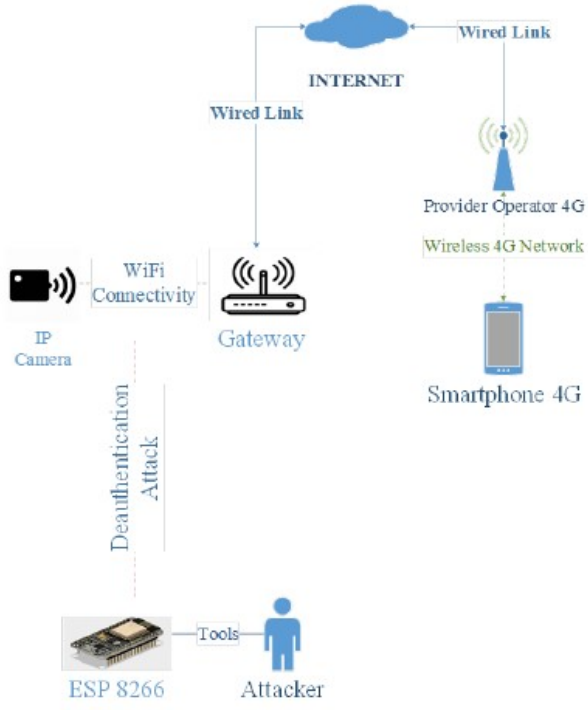

Fig. 4. Network diagram of deauthentication attack simulation with external test penetration.

Then, it scans the available Service Set Identifier (SSID), after finding the target to be attacked. Next, the deauthentication attack can be made. The programming script nowadays can be found on the Internet as deauther script.

Some parameters are needed to record the process during the test. First, it is the target or the media tested. Second, Basic Service Set Identifier (BSSID) is used to identify and enter the WiFi network. Third, it is Stands for Station (STA). It is a term for clients that are connected to WiFi network. Fourth, there are before and after attack status. Those are the status of the target before and after the attack. Fifth, the estimated time is the time of the attack carried out from the connected to the disconnected condition.

To record WiFi activities that are running, the researchers use CommView for WiFi V.7.0 from TamoSoft. The features provided are capturing every packet on the air to display important information such as access point and station's list per-node and perchannel statistics, signal strength, list of packages and network connections, protocol distribution graphs, and others. For more details, how the data is taken during the external penetration testing process is in **Fig. 5**.

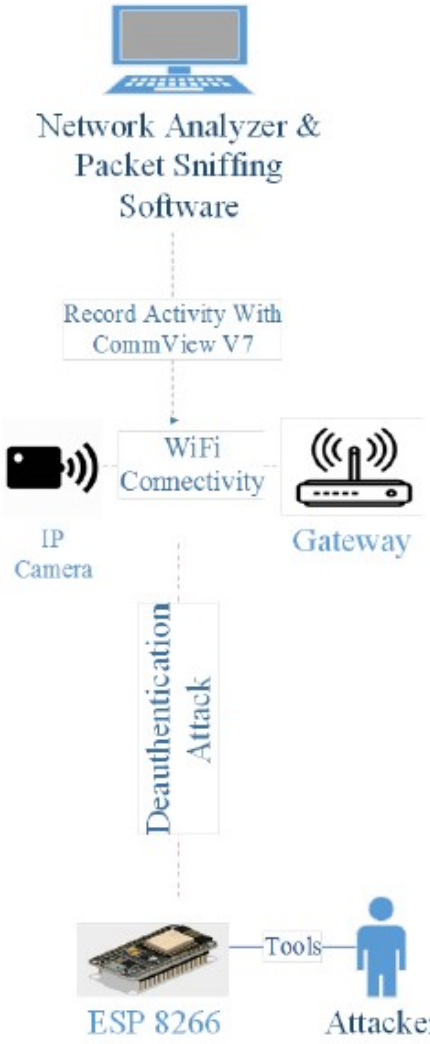

Fig. 5. Network diagram of the recording process during the external penetration test.

VIII. Required Components

The required components needed to complete this project is two. They are,

- NodeMCU ESP8266 module
- Micro USB cable

- **NodeMCU ESP8266**

NodeMCU is a low-cost open source IoT platform. It initially included firmware which runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which was based on the ESP-12 module.

The ESP8266 module enables micro controllers to connect to 2.4 GHz Wi-Fi, using IEEE 802.11 bgn. It can be used with ESP-AT firmware to provide Wi-Fi connectivity to external

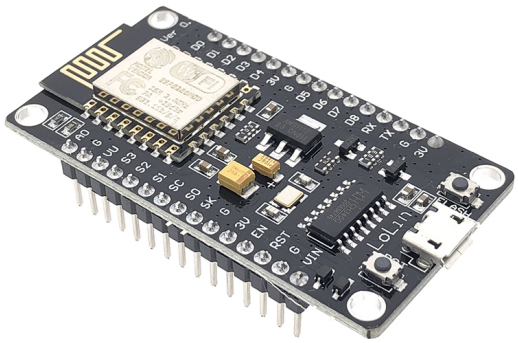

Fig. 6. NodeMCU ESP8266

host MCUs, or it can be used as a self-sufficient MCU by running an RTOS-based SDK. It can be seen in **Fig. 6**. It is the picture of a NodeMCU ESP8266. Arduino programming is used to configuring this micro controller device.

- **USB Cable**

The term USB stands for "Universal Serial Bus". USB is a standard port that helps to connect computer peripherals like scanner, printer, digital camera, flash drive and more to the Computer. The USB standard supports the data transfer at the rate of 12 Mbps. It can be seen in **Fig. 7**. It is the picture of a USB Cable.

Fig. 7. USB Device

The USB cable standard allows for these advantages over serial cable types:

- USB cables are "Hot Pluggable", in other words you can connect and disconnect the cables while the computer is running without fear of freezing the computer.
- USB cables are fast, transferring up to 480 Mbps. Compare to serial communication is about 20 Kbps.
- USB cables carry power as well as signals. This allows for "USB powered" gadgets as well as recharging batteries in cameras and other USB peripherals.
- USB cables are designed with several distinct connector types, making it easy to identify which plug goes into the computer and which plug goes into the peripheral device.
- USB cables are a universal standard and are fairly easy to find and to afford.

IX. Related Works

A. Update from the Board Manager

ESP8266 Boards Manager:
The ESP8266 is a low-cost Wi-Fi microchip, with built-in TCP/IP networking software, and micro controller capability, produced by Espressif Systems.
The firmware uses the arduino programming language (C Sharp). The firmware is based on the arduino project, and built on the Espressif Non-OS SDK for ESP8266. It uses many open source projects, such as Arduino-Json and Adafruit. **Fig. 8**

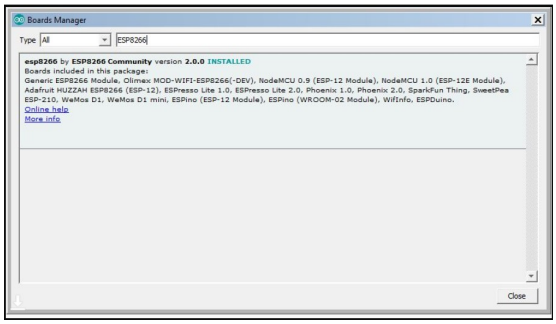

Fig. 8. Boards Manager

The procedure to install ESP8266 boards manager into arduino:

- Install Arduino and open it.
- Go to File, then to Preferences
- Add http://arduino.esp8266.com/stable/package-esp8266 to the Additional Boards Manager URLs.
- Go to Tools **>** Board **>** Boards Manager **>** Type in esp8266 **>** Select version 2.0.0 and click on Install.

B. Install Necessary Libraries

- Copy ESP8266Wi-Fi.cpp and ESP8266Wi-Fi.h
- Paste these files here packages > esp8266 > hardware > esp8266 > 2.0.0 > libraries > ESP8266WiFi > src

C. Upload Code to NodeMCU

- Open esp9266-deauther **>** esp8266-deauther.ino in arduino.
- Select your ESP8266 board at Tools **>** Board and the right port at Tools
  > Port If no port shows up you may have to reinstall the drivers.
- Adjust the Tools **>** Board **>** Verify the code **>** Upload the code **>** Check the serial monitor for successful connections.

D. Flow Chart of the Background process

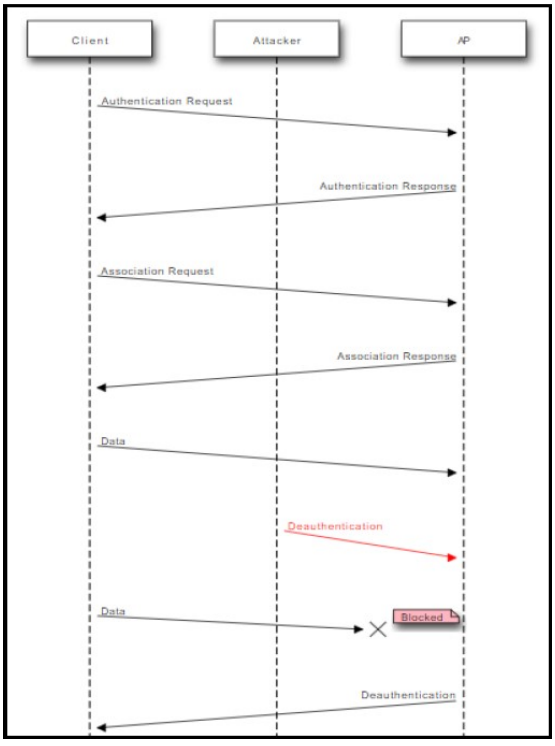

Fig. 9. Flow chart of the background process

X. Methodology

Here, it is discussed that how a **"WiFi Deauthering System"** works. After uploading the code, we will go to the IP address set up for the NodeMCU and system. Our set up IP address is **192.168.4.1**. After going to the address a warning page will be seen like **Fig. 10**.

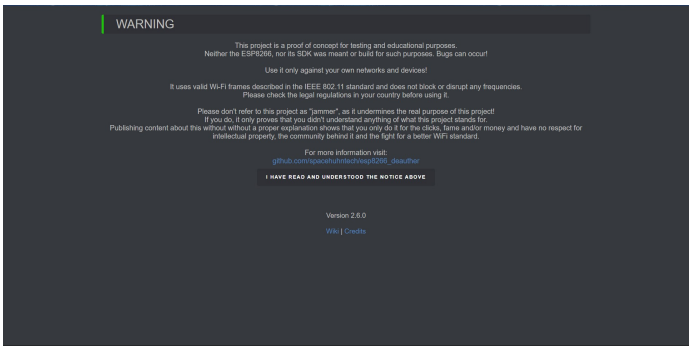

Fig. 10. Warning Page

After agreeing with the given instruction the main interface will be seen. There following things can be seen-

- A Scan Page
- A SSID Page
- An Attack Page
- A Settings Page

A. *Scan Page*

In the scan page all the Access Points stations near the deauther device can be seen. There we can select the access points or stations that we want to attack on. **Fig. 11**

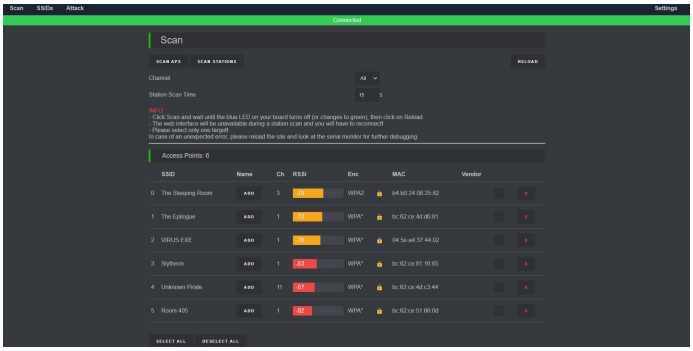

Fig. 11. Scan Page

In the scan page we can select multiple access points or stations or both at a time. We can also save access points and station for future use.

B. *SSID Page*

Here we can make clone of any specific access points or stations. We can create multiple clones by a specific name or random names. **Fig. 12**

In our system, we have used maximum 60 devices as cloning. We tap the beacon option to perform cloning.

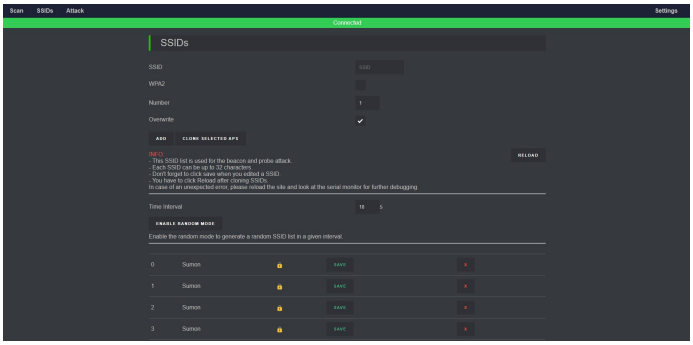

Fig. 12. SSID Page

C. *Attack Page*

In the attack page, we perform the deauth function, beacon function probe function. **Fig. 13**

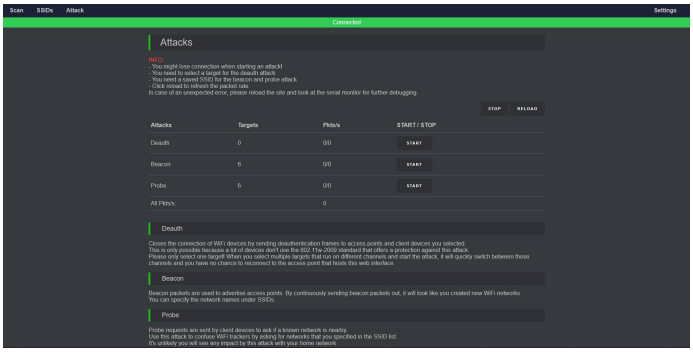

Fig. 13. Attack Page

Deauth function is used to disconnect the selected access points stations. Beacon function is used to create clones. Probe is used to change the ssid list after a limited time interval.

D. *Settings page*

The settings page allows the system user to change the device's ssid, password or the IP address. **Fig. 14**

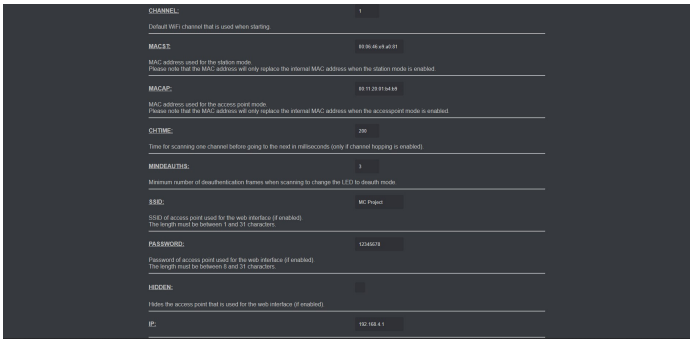

Fig. 14. Settings page

Here we can also change the option where we can also select whether the WiFi system will be hidden or visible.

XI. Implementation Results

We have implemented the system and have performed the deauthing and beacon in the attack page.

Firstly, we have selected the access points we want to perform the features on. **Fig. 15**

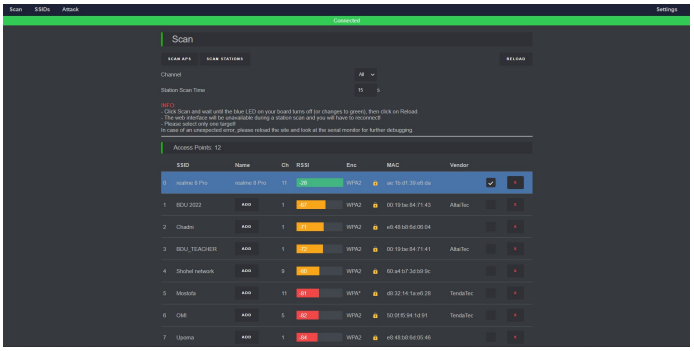

Fig. 15. Select The Access Point

the selected device will be added to the favourite list if we add the device. We can perform the deauth function in the attack section. **Fig. 16**

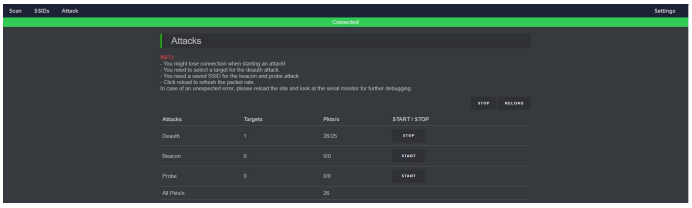

Fig. 16. Start Deauth operation

When we start the deauth function one can't connect to that network anymore.It will show **"connecting"** but it will not connect even if one tries to forget the network and give correct password. **Fig. 17**

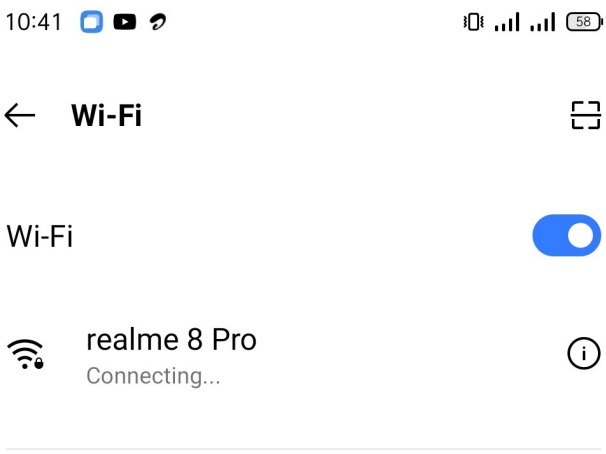

Fig. 17. WiFi shows connecting but does not connect

If we want to perform cloning of the selected access point then firstly we go to the ssid page and select the cloning option and reload the system. There creates 60 fake ssid of the selected access point. We can cross and keep how many clones we want to create. **Fig. 18**

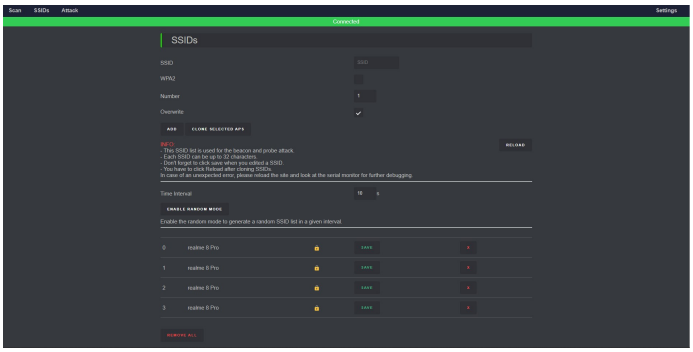

Fig. 18. Create cloning

Then we go to the attack page and select beacon or probe. When we press the beacon option and start the operation it creates the specific amounts of clones that we have set up in the ssid page. There will be created some clones. **Fig. 19**

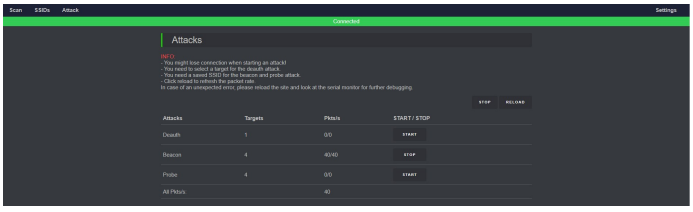

Fig. 19. Start the Beacon operation

After we start the beacon operation we will see a specific amount of WiFi with same name that has been set in the WiFi

section in any device. Here we have set 5 WiFi clones. **Fig. 20**

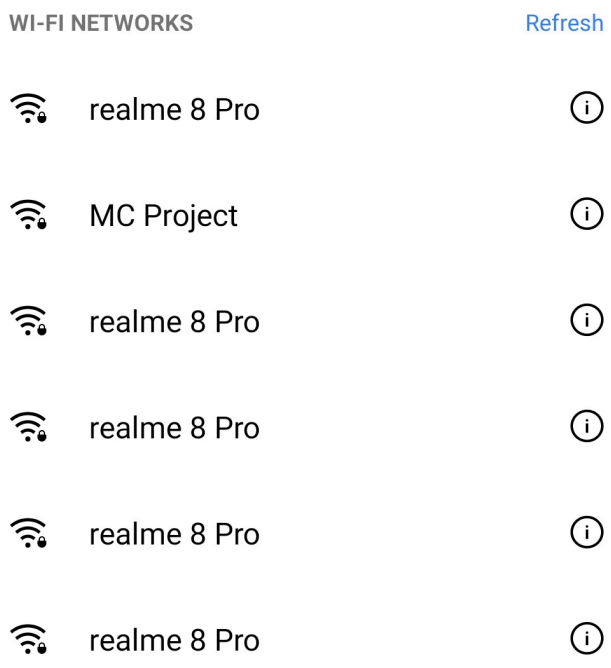

Fig. 20. Clones got created of a specific WiFi

XII. Conclusion

The most useful packets the Wi-Fi Deauther is able to create are deauthentication and disassociation packets. These special packets are often abused because they are unauthenticated, meaning anyone on a network can send them to anyone else while pretending the messages are coming from the router. When a device on the Wi-Fi network receives the packet, it immediately disconnects from the network. The Wi-Fi Deauther does this over and over, spamming connected devices with "disconnect" messages. This results in a "jamming" effect on the network as devices cannot connect fast enough to avoid being instantly kicked off.

This isn't the only trick the Deauther program has up its sleeve. It's also capable of scanning for both nearby access points and connected devices, and cloning any Wi-Fi network it sees. It can also generate dozens of fake Wi-Fi networks with any names you want, monitor channels for packet traffic between devices, and do all of this from a fancy built-in web interface.

XIII. Future Scope

- **Evil Twin Access point**

One of the main purposes of deauthentication used in the hacking community is to force clients to connect to an Evil twin access point which then can be used to capture network packets transferred between the client and the RAP.

The attacker conducts a deauthentication attack to the target client, disconnecting it from its current network, thus allowing the client to automatically connect to the Evil twin access point.

This type of attack may be used to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves setting up a fraudulent web site and luring people there. [1]

- **Password Attacks**

In order to mount a brute-force or dictionary based WPA password cracking attack on a WiFi user with WPA or WPA2 enabled, a hacker must first sniff the WPA 4-way handshake. The user can be elicited to provide this sequence by first forcing them offline with the deauthentication attack.

In a similar phishing style attack without password cracking, Wifiphisher starts with a deauthentication attack to disconnect the user from his legitimate base station, then mounts a man-in-the-middle attack to collect passwords supplied by an unwitting user.

References

[1] Wolfe, Daniel (February 14, 2007). "Security Watch". American Banker. 172 (31). New York, NY. p. 7. ISSN 0002-7561. Retrieved 18 Oct 2016 – via ProQuest. A security firm used an evil twin as a test to obtain passwords from attendees at an RSA security conference

[2] A. Efe, E. Aks¨oz, N. Hanecio˘glu, and S¸ . N. Yalman, "Smart security of IoT against DDOS attacks," International Journal of Innovative Engineering Applications, vol. 2, no. 2, pp. 35–43,2018.

[3] E. Oriwoh and G. Williams, "Internet of Things: The argument for smart forensics," in Handbook of research on digital crime, cyberspace security, and information assurance. USA: IGI Global, 2015, pp. 407–423.

[4] P. Thornycroft. (2016) Wi-Fi access for the Internet of Things can be complicated. [Online]. Available: https://bit.ly/3cv2UqI

[5] M. Bogdanoski, P. Latkoski, and A. Risteski, "Analysis of the impact of AuthRF and AssRF attacks on IEEE 802.11e-based access point," Mobile Networks and Applications, vol. 22, no.5,pp. 834–843, 2017.

[6] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 6, pp. 383–388, 2017.

[7] C. Liu and J. Qiu, "Performance study of 802.11w for preventing DoS attacks on wireless local area networks," Wireless Personal Communications, vol. 95, no. 2, pp. 1031–1053, 2017.

[8] J. Milliken, V. Selis, K. M. 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.

[9] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, pp. 355–373, 2018.

[10] T. Khalil, "IoT security against DdoS attacks using machine learning algorithms," International Journal of Scientific and Research Publications, vol. 7, no. 6, pp. 739–741, 2017.

[11] M. Alamanni, Kali Linux wireless penetration testing essentials. UK: Packt Publishing, 2015.

[12] Course Technology Cengage learning, Penetration testing procedures methodologies. USA: Nelson Education, Ltd., 2011.

[13] H. Ikasamo. (2018) ESP8266/ESP32 connect WiFi made easy. [Online]. Available: https://www.hackster.io/hieromon-ikasamo/esp8266-esp32-connect-wifi-made-easy-d75f45