Wi-fi Deauthenticator and Detector

TEAM 17:

- Kuljeet Singh Bhengura
- Kevin Dsouza
- Disha Sanil

PROBLEM STATEMENT

The objective of this paper is to investigate and perform a special type **Denial of Service (DoS)** attack against 802.11 wireless networks. This attack is known as the **Deauthentication Attack** which is launched against 802.11-based wireless networks. When any wireless access point wants to disconnect a client or all the connections are terminated, it sends special frames known as deauthentication or disassociation frames. Due to being **unencrypted**, these frames do not require an authenticated user. Hence, we as attackers can craft these frames and send them to the access point in such a way that the access point assumes the frames to be coming from the client and not the attacker. This attack can be launched easily using minimal resources.

In this project, we also present an efficient solution on **Detecting** the Deauthentication attacks.Our proposed module is lightweight and detects the attack with high accuracy & low false positive rate. Our technique can be easily deployed on open as well as encrypted networks. The module works for both **Deauthorization Attacks** and **Disassociation Attacks.** Therefore, we carry out an o**ffence and defence** strategy.

SCOPE OF THE PROJECT GOAL

OFFENCE:

1.One place where deauthentication can be particularly useful is at a school or university. By blocking cell phone signals, students cannot become distracted by their phones. In addition, they cannot cheat by sending text messages to one another during exams.

2.High security premises, such as prisons and detention centers, can also benefits from a jammer because it can prevent illicit communication between inmates and visitors.

3.Of course, a cell phone jammer can also be beneficial in places such as a movie theater or a library where other patrons expect silence so they can enjoy their activities.

SCOPE OF THE PROJECT GOAL

DEFENCE:

Since wireless local area network (WLAN) management frames are often unencrypted, an attacker can potentially attack the WLAN infrastructure by spoofing the Media Access Control (MAC) address of a client device that is associated with the WLAN, and sending a deauthentication and/or disassociation frame using the MAC address of the associated client device. Because the WLAN infrastructure cannot determine that the deauthentication and/or disassociation frame is from an attacker or a valid client device, it will terminate the client device's connection to the WLAN. As a result, a valid client device will experience denial of service by the WLAN infrastructure.

SCOPE OF THE PROJECT FEATURES

1) Features of the Deauther

2) Features of the Deauth Detector

LITERATURE SURVEY:
Offence

1) Signal Jamming

The most basic form of DoS attack is when another signal interferes with data transmissions as shown. Such interference can occur continuously or intermittently and arise from a variety of sources apart from malicious activity.

2) Disassociation Attack

A very similar vulnerability may be found in the association protocol that follows authentication. The IEEE 802.11 standard allows clients to associate with only one AP at a time.

3) Continuous Collision Jamming

Continuous collision jamming is effective but relatively expensive in energy terms and increases the probability that the attacker's location will be discovered. The study of Karhima et al. considered the effectiveness of continuous jamming signals against IEEE 802.11"b" and "g" networks [].

4) Resource Depletion Attacks

Resource Depletion Attacks Resource depletion attacks normally target shared resources such as the AP to exhaust its processing and memory power so that it can no longer provide services to other (legitimate) stations. These attacks can be accompanied by more sophisticated attack such as introducing rogue access points to hijack the abandoned stations.

LITERATURE SURVEY:
Defence

1) Pseudo-Randomised Sequence Number

This study suggests a Pseudo Randomized sequence Number based solution to 802.11 Disassociation DoS attack. He suggests that the solution does not require any additional hardware and can be implemented in both wireless clients and Access Point via firmware upgrade. It was just mathematically implemented not physically.

2) Analysis and improvements of PEAP protocol

This paper showed that in recent years a large number of applications are developed for WLAN. But different types of issues related to security are also coming in WLAN. To provide security we need a secure authentication protocol like PEAP. This paper mainly talks about Protected Extensible Authentication Protocol (PEAP). The main concerns are its authentication process, what are the defects in EAP-PEAP and how we can improve PEAP so it can overcome through these defects

3) Static 4-Way Handshake

Floriano De Rango *et. al.*, [] proposed static and dynamic 4 - way handshake solutions to avoid denial of service attack in WPA and IEEE 802.11i.

4) A Survey on Wireless Security protocols

This study presented a survey on wireless security protocols (WEP, WPA and WPA2/802.11i). Here WEP protocol types, weaknesses and enhancements, WPA protocol types, Cryptographic messages. Finally paper explained third generation of wireless security protocol as WPA2/802.11i.

LITERATURE SURVEY:

TYPES OF DOS ATTACKS AND COUNTERMEASURES

Attack	Target	Existing countermeasures
Probe Request Attack	AP	Signal Print
Authentication Request Attack	AP	Signal Print, Client Puzzle
Deauthentication Attack	Station and AP	Signal Print, MAC Spoof Detection, Delaying the effects of request
Association Request Flood	AP	Signal Print
Deassociation Attack	Station and AP	Signal Print, MAC Spoof Detection, Delaying the effects of request
Virtual Carrier Sense Attacks	Medium Access	Explainability of Collision, Spatial Retreats
Sleeping Node Attack	Station and AP	Limiting Duration Field Value, Signal Print, MAC Spoof Detection

REQUIREMENTS SPECIFICATION

HARDWARE REQUIREMENTS:

1.NodeMCU x 2

2.RGB LEDS x 2

3.OLED 0.96” I2C - IIC Interface

4.BUTTONS (TACTILE ON/OFF SWITCH)

5. BREADBOARDS x 3

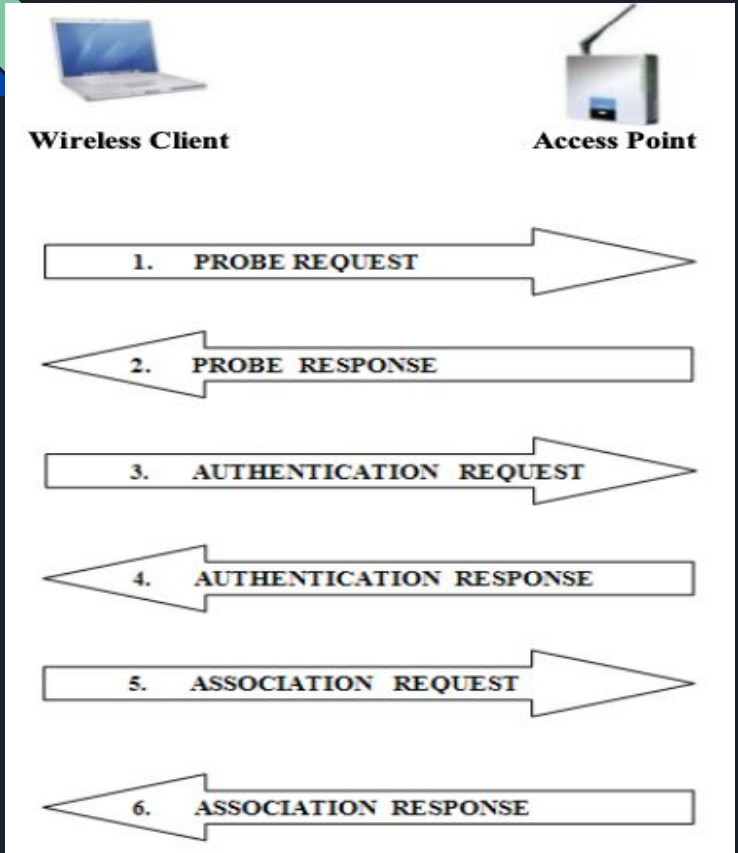
6. JUMPER WIRES

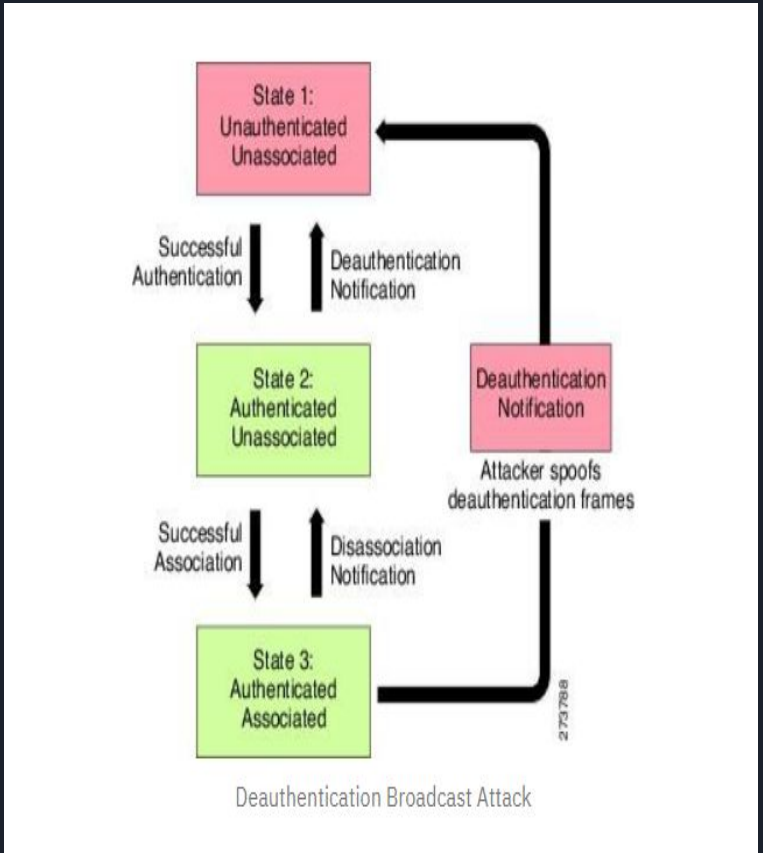
7. POWER SUPPLY/ BATTERY

SOFTWARE REQUIREMENTS:

1)Arduino IDE

SCHEMATIC DIAGRAM





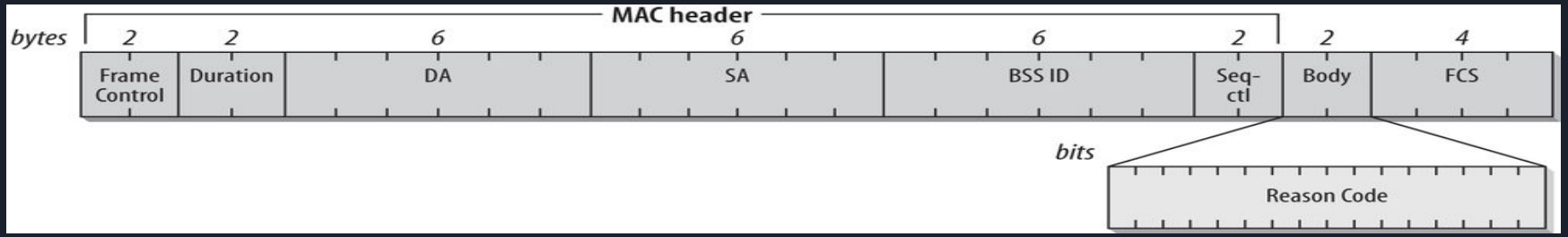
CONCEPTUAL EXPLANATION

There are **three** major types of frame used in IEEE 802.11 networks:

1) **Data Frames**: Data frames carry higher-level protocol data in the frame body.

2) **Control Frames**: Control frames assist in the delivery of data frames by providing area-clearing operations, channel acquisition and carrier-sensing maintenance functions, and MAC-layer reliability functions.

3) **Management Frames**: Management frames perform supervisory functions; they are used to join and leave the wireless network and move associations from access point to access point.



Body of Deauthorization Frame

Detection of Deauthentication Frame:

(wlan.fc.type == 0) AND (wlan.fc.type_subtype == 0x0c)

Detection of Disassociation Frame:

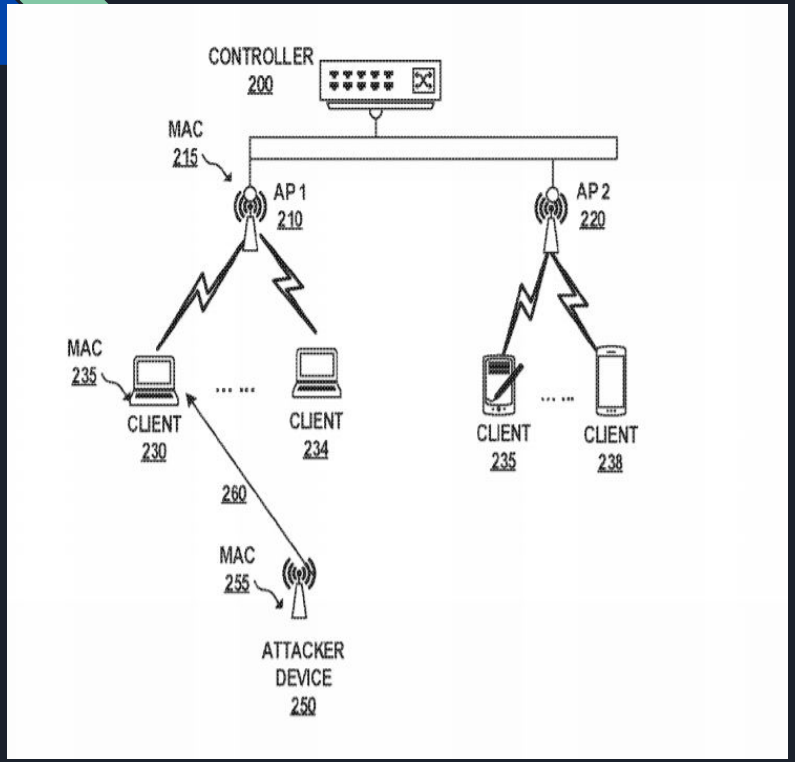
(wlan.fc.type == 0) AND (wlan.fc.type_subtype == 0x0c)

DIFFERENCE BETWEEN OUR DEAUTHER AND A WIFI JAMMER

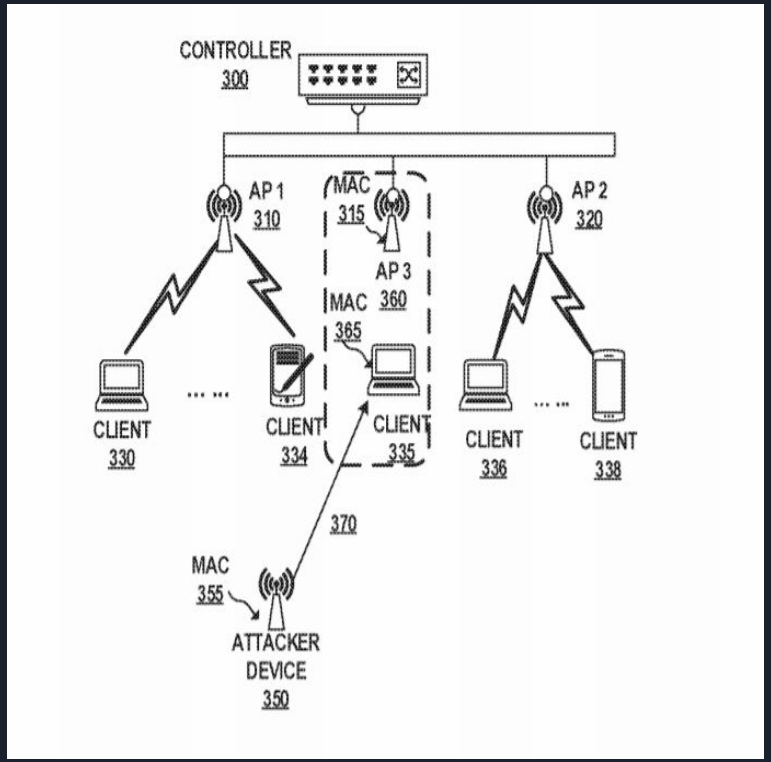
Wifi Jammer vs Team 17 Deauther

WIFI JAMMER	TEAM 17'S DEAUTHER
Creates noise on a specific frequency range (i.e. 2.4GHz)	Exploits a particular **vulnerability** of IEEE 802.11 Standards
Targets **Frequency Bands**. Eg: 2.4GHz or 5GHz Band	Targets particular **Access Points** only
All Wifi's on the same frequency get jammed	All Wifi's **do not** get affected. Only the Target AP and Clients are affected
Mostly **ILLEGAL** to use	Mostly **LEGAL** to use
Increases the Noise:Signal Ratio. Therefore, AP is not ACCESSIBLE	Does not affect the Noise:Signal Ratio. AP is reachable but Client thinks AP sends a Deauth Signal
EXPENSIVE	MUCH CHEAPER

WORKING OF THE MODULES

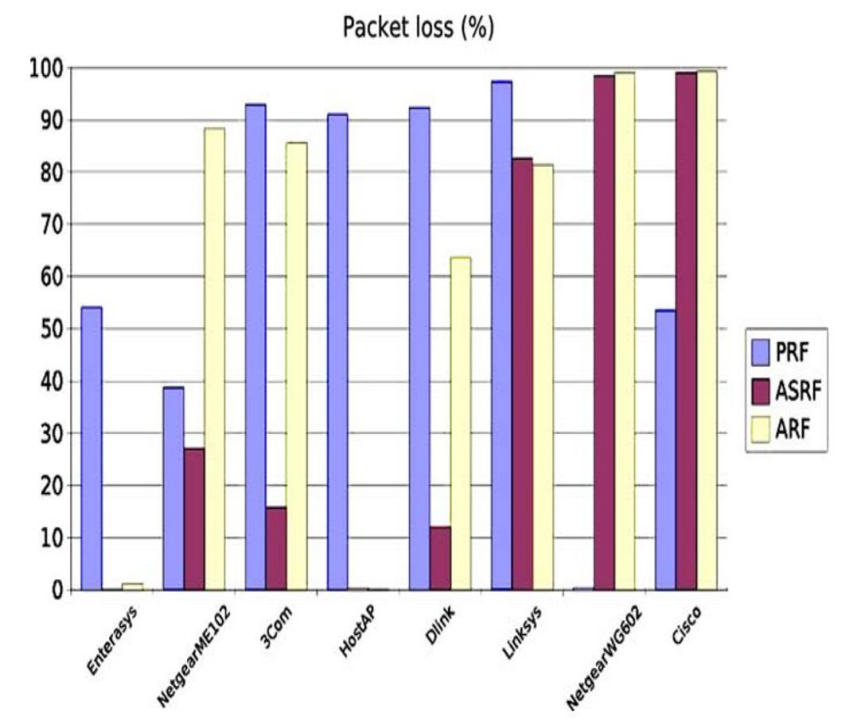


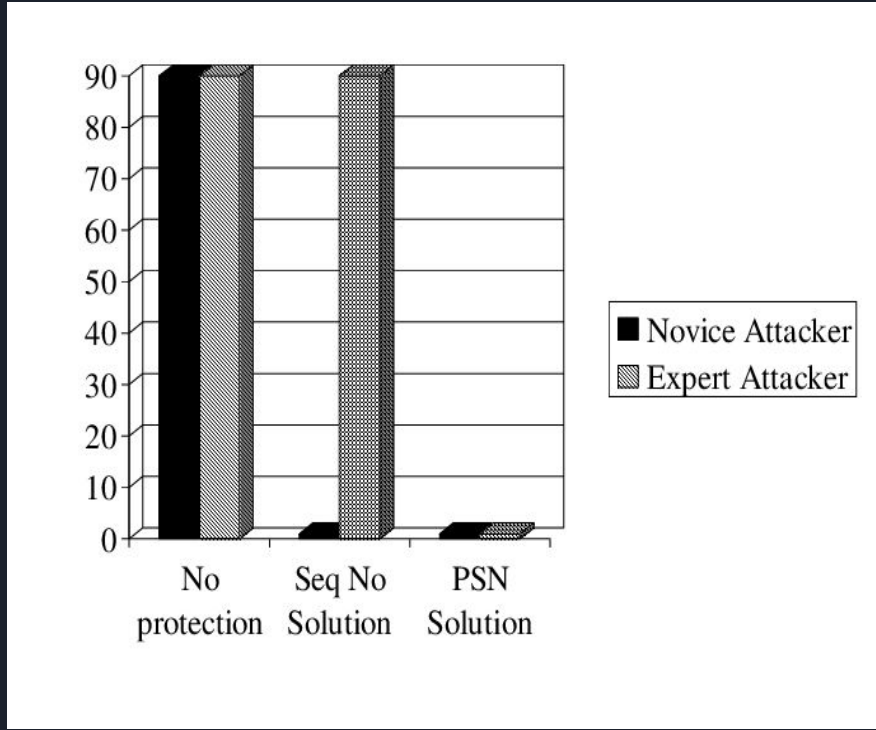
DEAUTH ATTACK



DEAUTH ATTACK DETECTION

ACCURACY OF THE ATTACK AND DETECTION



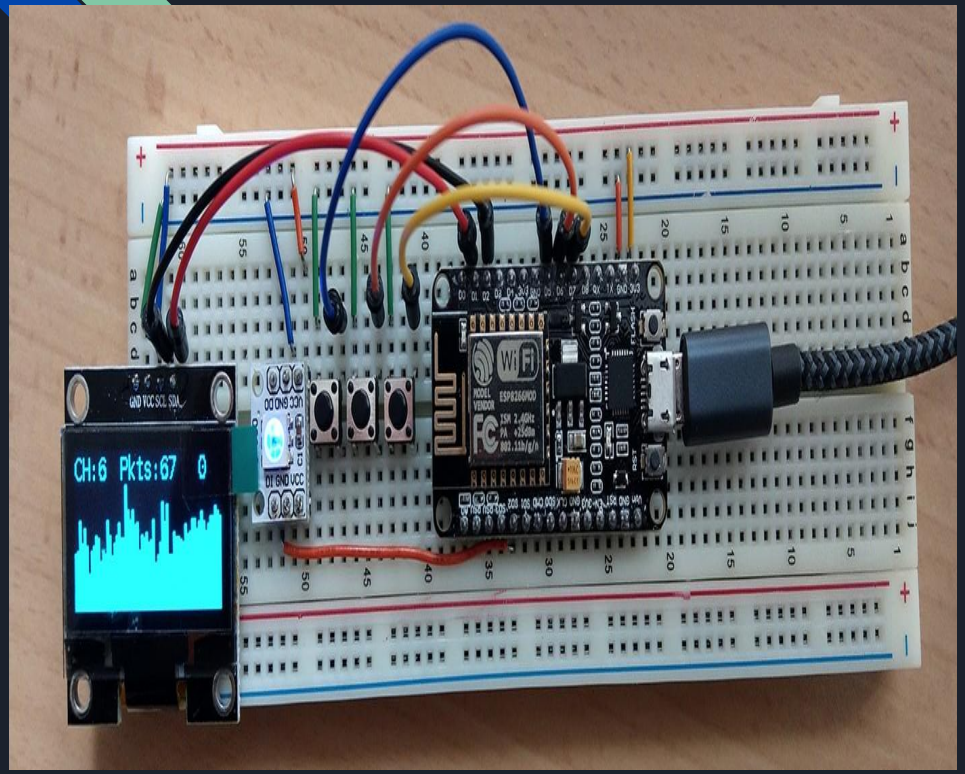


DEAUTH ATTACK %

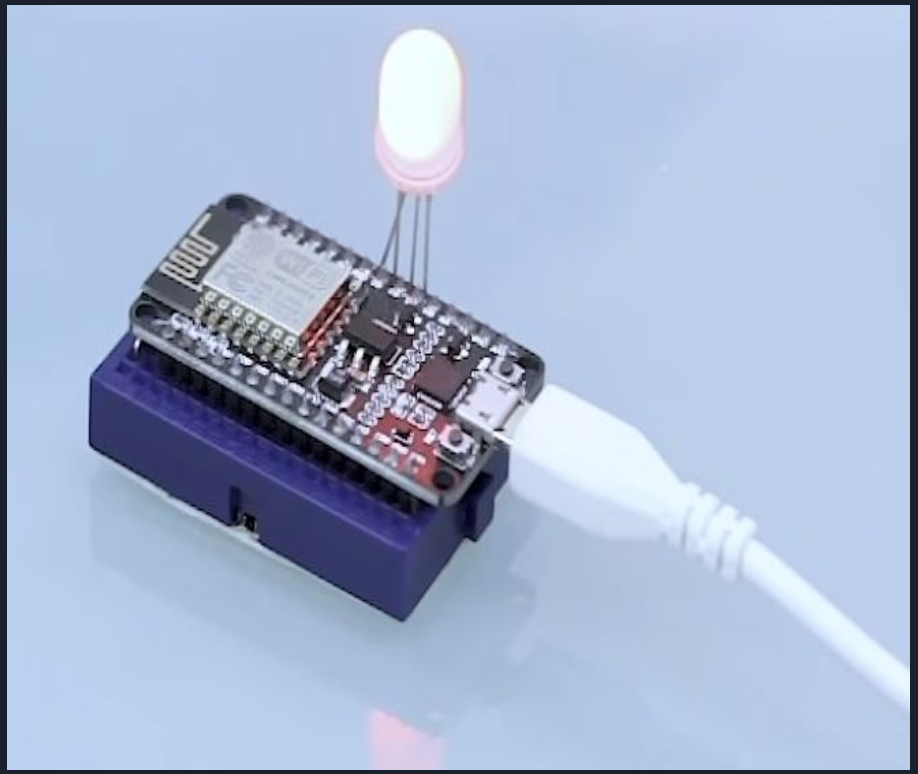
DEAUTH ATTACK DEFENCE %

**PRF: Probe Request Flood, ARF: Authentication Request Flood (ARF), ASRF: Association Request Flood (ASRF).*

IMPLEMENTATION



DEAUTHENTICATOR



DEAUTH DETECTOR

PROJECT PLAN

REFERENCES