# Wi-Fi Deauthenticator and Deauth Detector

TEAM 17:

- Kuljeet Singh Bhengura
- Kevin Dsouza
- Disha Sanil

Guide: Prof. Prasad Padalkar

# PROBLEM STATEMENT

1) There are many *security risks* associated with the current wireless protocols (IEEE 802.11 Protocols) and encryption methods.
2) Students and Employees using Wi-Fi Hotspots in the working zone and, therefore, losing focus.
3) Usage of  Wifi controlled weapons, bots and bombs in critical regions.

# SCOPE OF THE PROJECT
# GOAL

**OFFENCE**:

1. One place where deauthentication can be particularly useful is at a *School or a University*

2. High security premises, such as prisons and detention centers

3. In Military Services

4. Help achieve quiet and silence in a conference/meeting room.

# SCOPE OF THE PROJECT
# GOAL

DEFENCE:

1) Detect Wireless Deauthentication or Disassociation Attack

2) Indicate different attacks with different colors for clarity

2) Create awareness about 802.11w

# FEATURES OF THE DEAUTHER

1) Once your Wi-Fi Deauther board is powered, you shouldn't need a screen to interact with it.

2) The first page you'll find yourself on is the "Scan" page, which breaks down results into a few easy to understand categories.

3) Select Target Networks

4) Launch an Attack

5) Attacks can be Deauth, Beacon or Probe

# FEATURES OF THE DEAUTH DETECTOR

1) We can define whether or not we want to Channel Hop or just stay on one channel by setting the "channelHopping" setting to "true."

2) Next, we have a series of variables which keep track of things in the script.

3) Next, we have a sniffer function, and an "if" statement that adds to the "c" counter

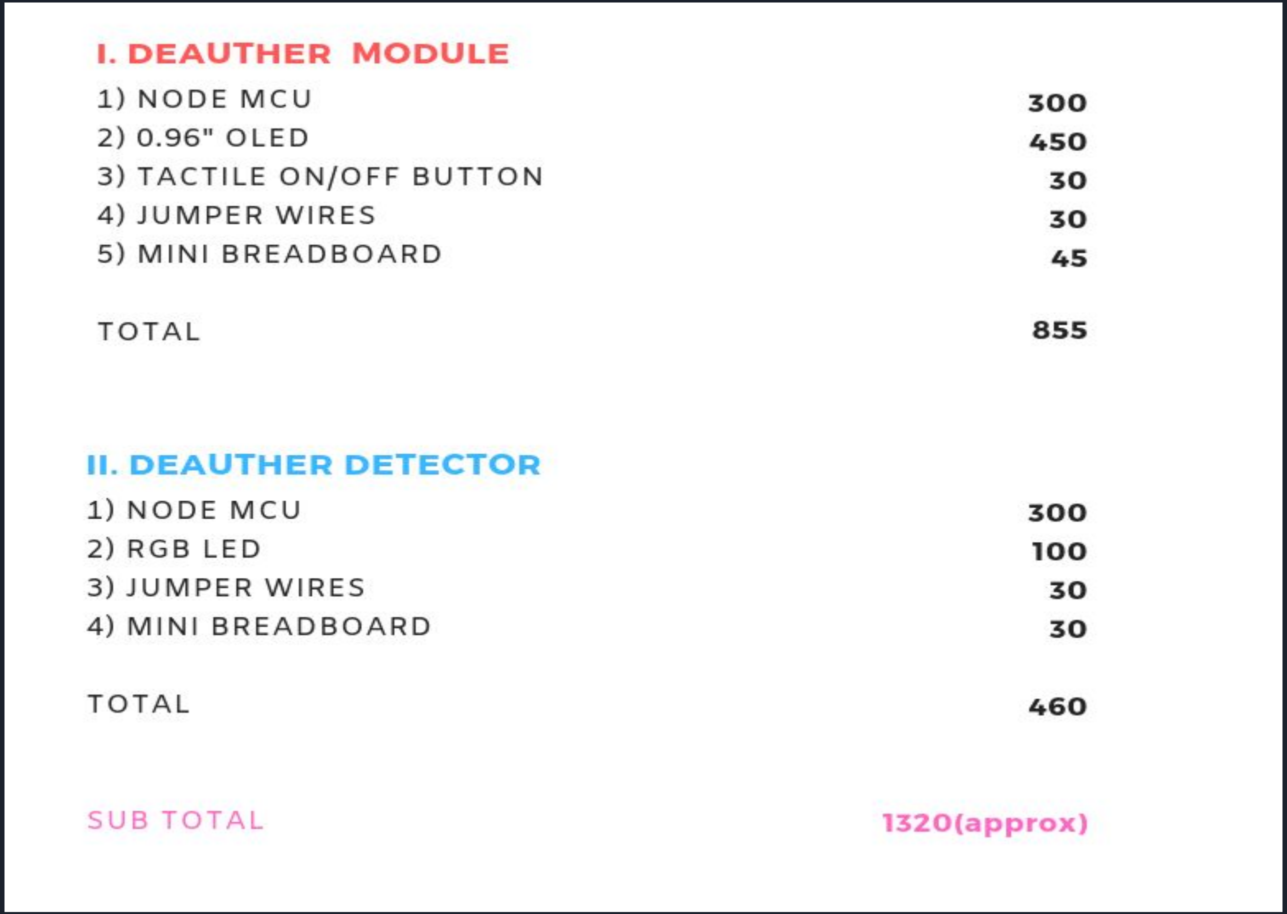
4) We insert two "if" statements that will add to a cooldown timer.

5) Whenever we detect Disassociation/Deauth packets, we'll turn on an LED by setting the cooldown timer to 500

```
if(buf[12] == 0xA0){dissoc = 500;}
if(buf[12] == 0xC0){deauth = 500;}
```

5) Now, our module decides what happens when the packet doesn't match, meaning it's a normal Wi-Fi packet and not one we're looking for.

# COST OF PROJECT



## I. DEAUTHER MODULE

| | |
|---|---|
| 1) NODE MCU | 300 |
| 2) 0.96" OLED | 450 |
| 3) TACTILE ON/OFF BUTTON | 30 |
| 4) JUMPER WIRES | 30 |
| 5) MINI BREADBOARD | 45 |
| TOTAL | 855 |

## II. DEAUTHER DETECTOR

| | |
|---|---|
| 1) NODE MCU | 300 |
| 2) RGB LED | 100 |
| 3) JUMPER WIRES | 30 |
| 4) MINI BREADBOARD | 30 |
| TOTAL | 460 |

| | |
|---|---|
| SUB TOTAL | 1320(approx) |

# 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].

**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

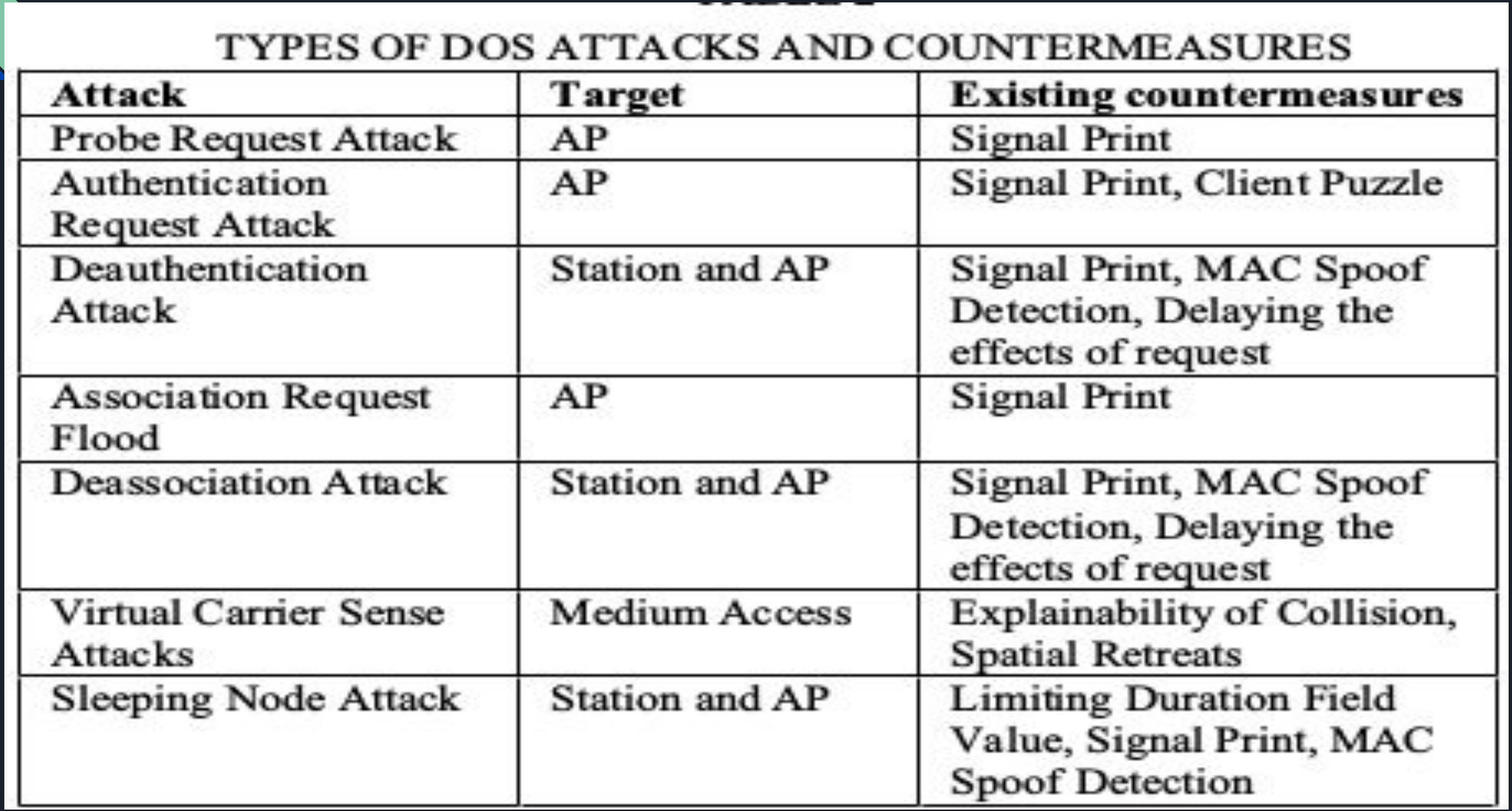
## 3) Static 4-Way Handshake

Floriano De Rango *et. al.*, [5] 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.

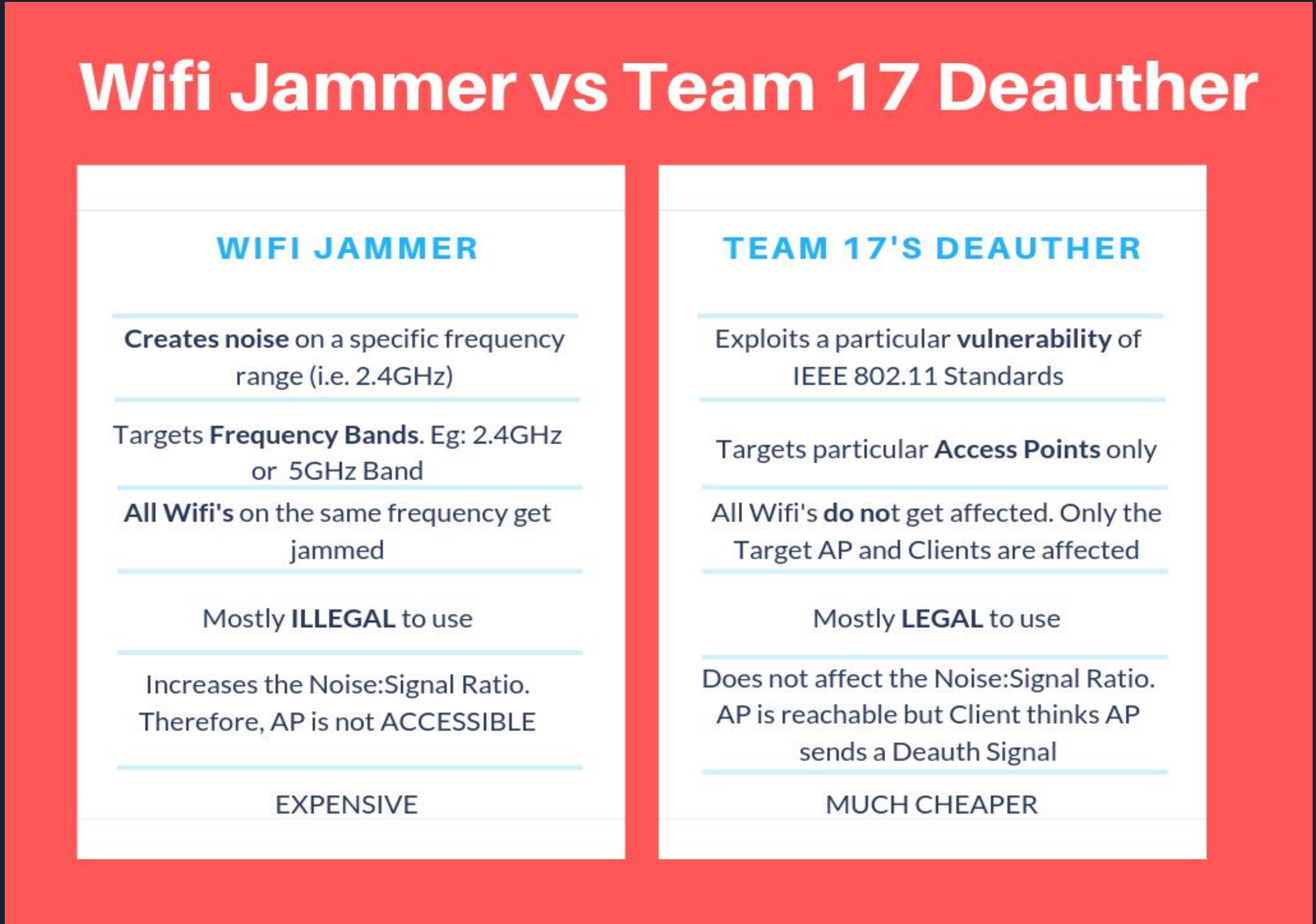
# LITERATURE SURVEY:



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 |

# DIFFERENCE BETWEEN TEAM 17’s 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 |

# REQUIREMENTS SPECIFICATION

## HARDWARE REQUIREMENTS:

1.NodeMCU x 2

2.RGB LEDS

3.OLED 0.96”  I2C - IIC Interface

4.BUTTONS (TACTILE ON/OFF SWITCH)

5. BREADBOARDS x 3

6. JUMPER WIRES

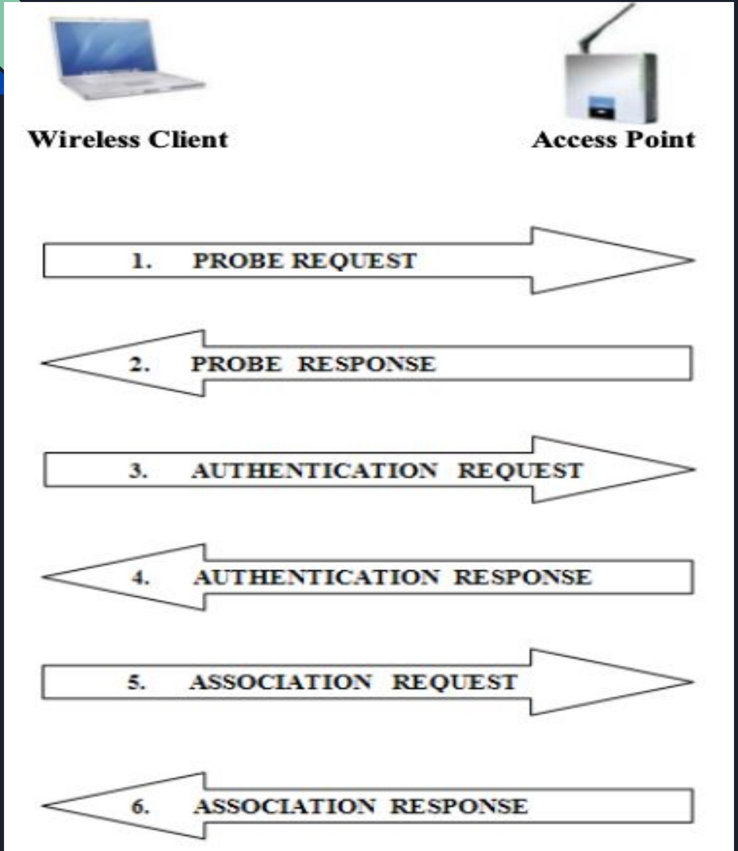
7. POWER SUPPLY/ BATTERY

## SOFTWARE REQUIREMENTS:

1)Arduino IDE

2) HTML to HEX Converter

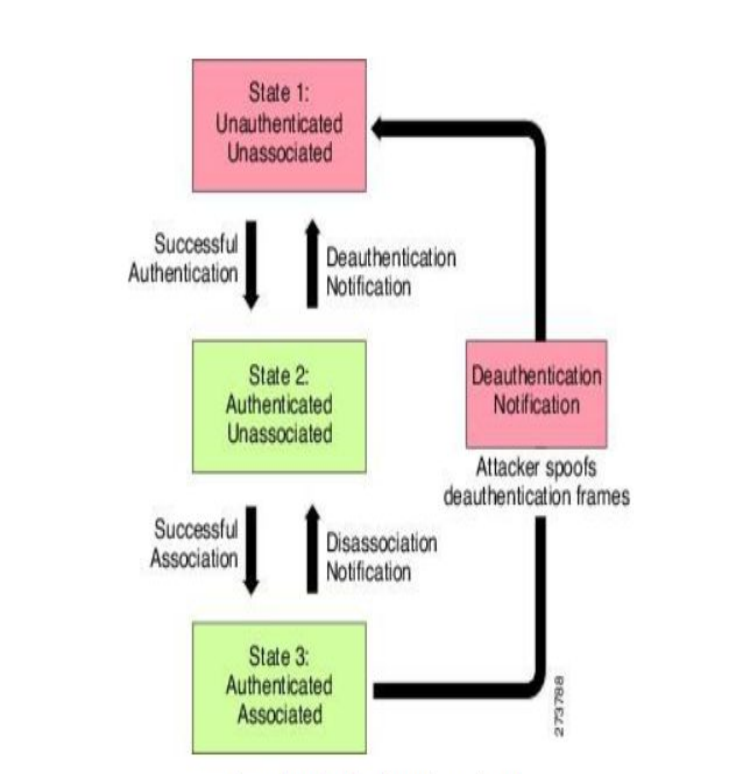
# SCHEMATIC DIAGRAM



Wireless Client

Access Point

1. PROBE REQUEST
2. PROBE RESPONSE
3. AUTHENTICATION REQUEST
4. AUTHENTICATION RESPONSE
5. ASSOCIATION REQUEST
6. ASSOCIATION RESPONSE



State 1: Unauthenticated Unassociated

Successful Authentication

Deauthentication Notification

State 2: Authenticated Unassociated

Successful Association

Disassociation Notification

State 3: Authenticated Associated

Deauthentication Notification

Attacker spoofs deauthentication frames

Deauthentication Broadcast Attack

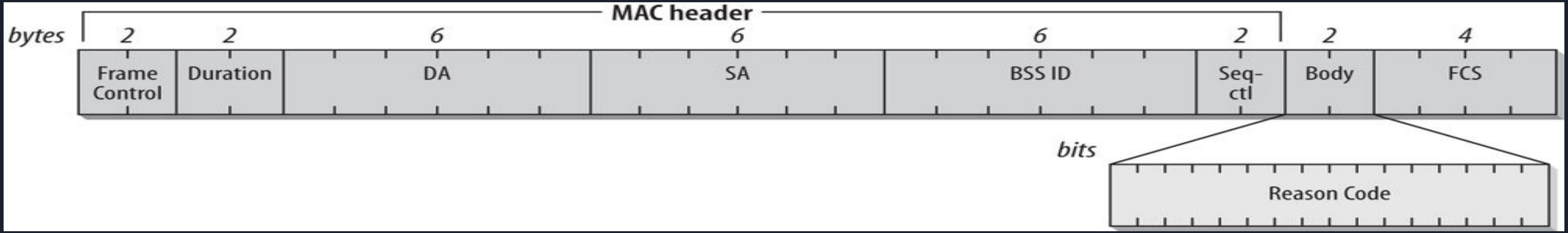
# CONCEPTUAL EXPLANATION

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. Example: CTS, ATS, ACK

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*

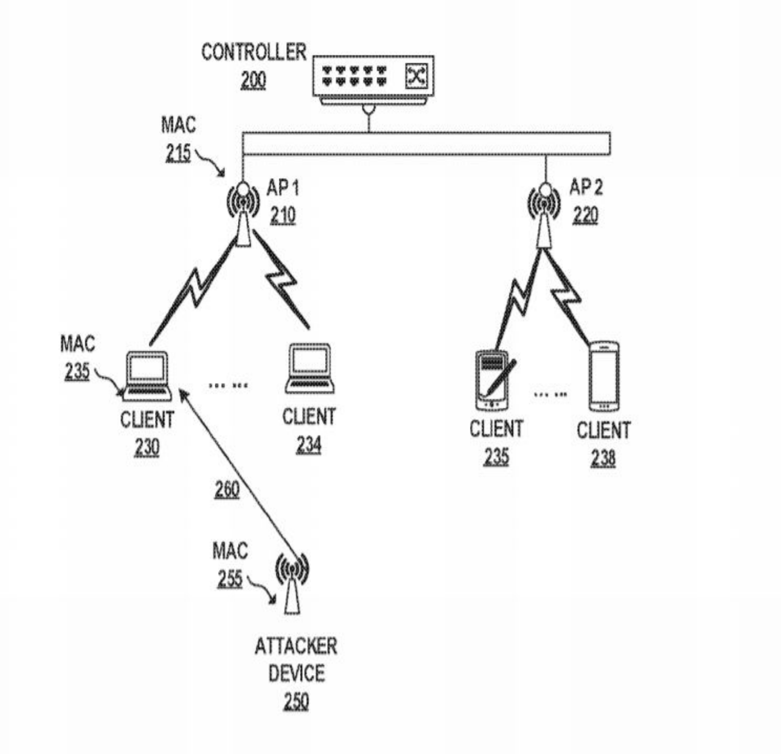
Detection of Deauthentication Frame:

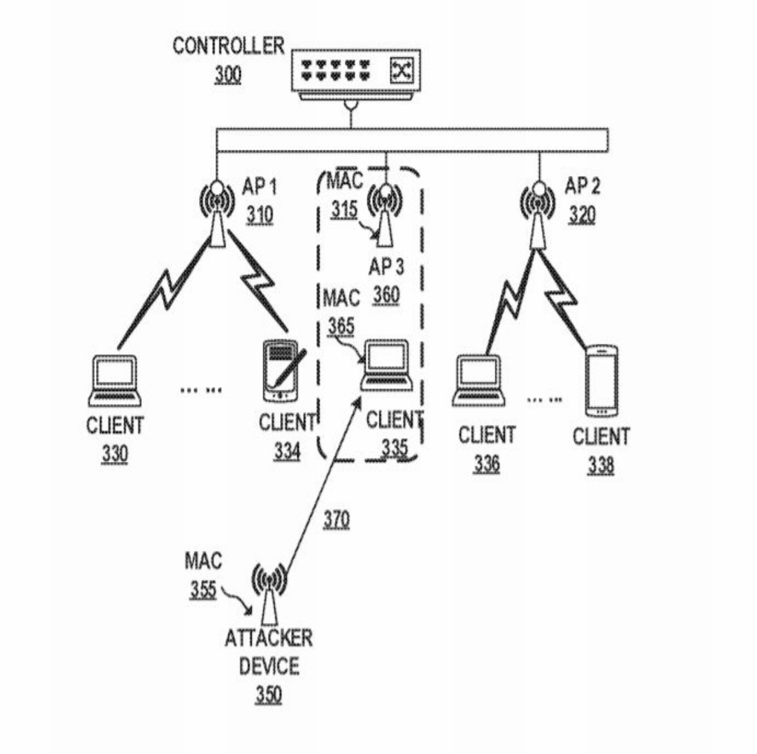
(wlan.fc.type == 0) AND (wlan.fc.type_subtype == 0x0c)

Detection of Disassociation  Frame:

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

# WORKING OF THE MODULES

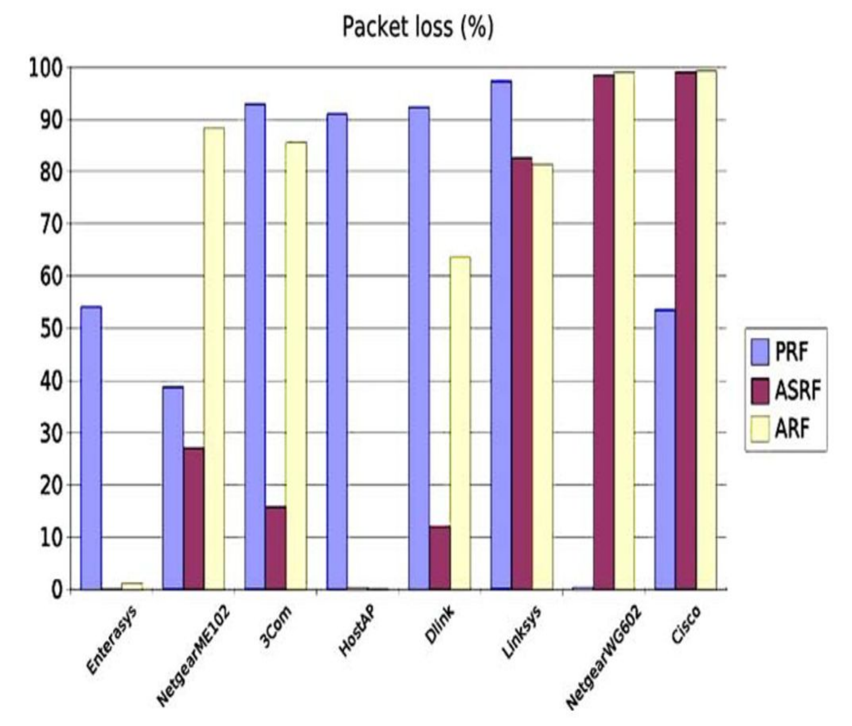


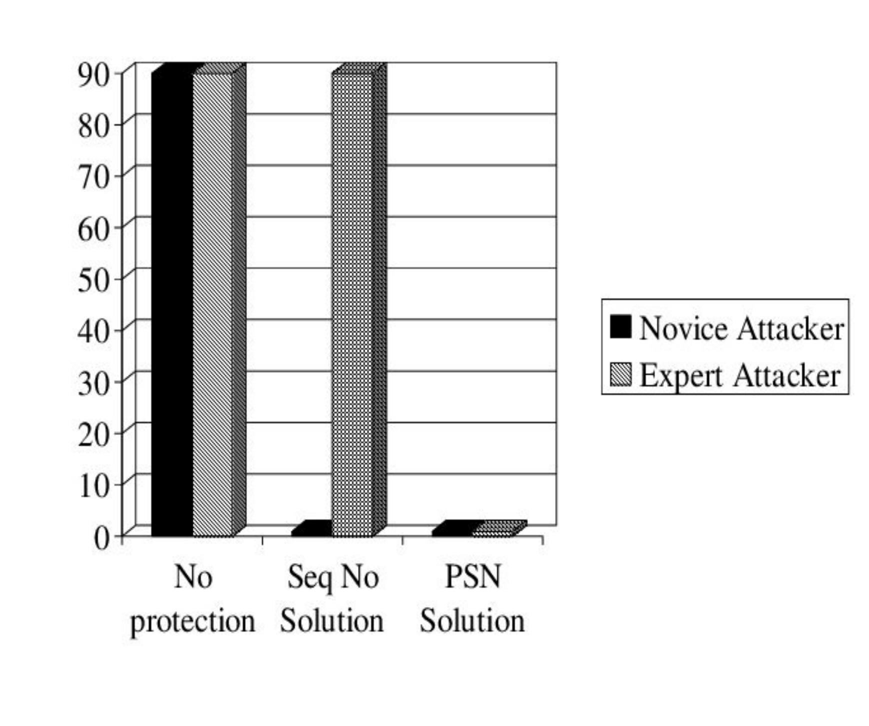


<u>DEAUTH ATTACK</u>

<u>DEAUTH ATTACK DETECTION</u>

# ACCURACY OF THE ATTACK AND DETECTION



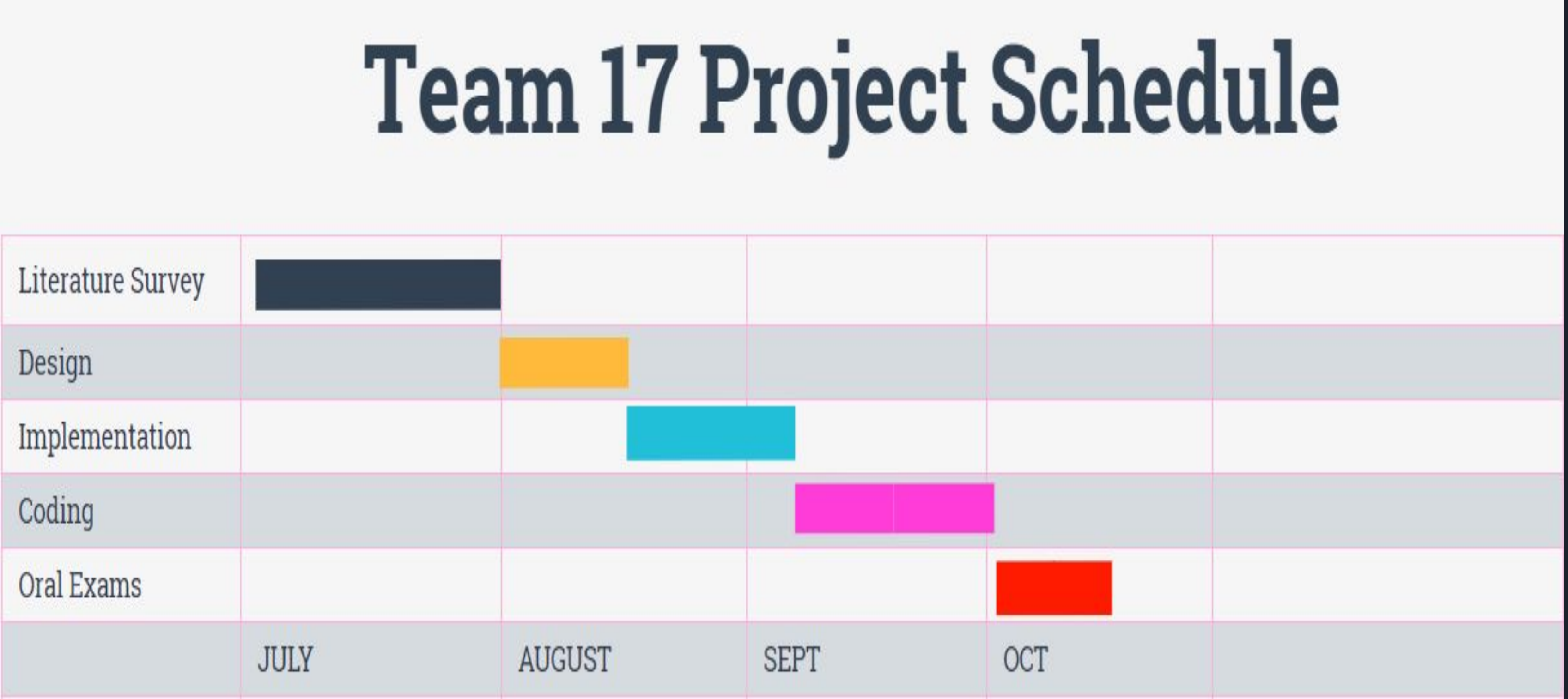


DEAUTH ATTACK %

DEAUTH ATTACK DEFENCE %

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

# PROJECT PLAN



Team 17 Project Schedule

# REFERENCES

[1] A. Atul, "Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks," MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking, pp. 30-44.

[2] M. Bernaschi, F. Ferreri, and L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks," Wirel. Netw., vol. 14(2), pp. 159-169, 2008.

[3] Prabhaker Mateti, The Handbook of Information Security. Dayton: John Wiley & Sons, Inc, 2005.

[4] Teemu Karhima, Aki Silvennoinen, Michael Hall, and Sven-Gustav Häggman. IEEE 802.11b/g WLAN tolerance to jamming. In *IEEE Military Communications Conference, 2004*, volume 3 of *MILCOM 2004*, pages 1364–1370, October 2004.

[5] De Rango, Floriano, Cristian Lentini, Dionigi, Marano, Salvatore, EURASIP Journal on Wireless Communications and Networking, “Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i”, 2006

[6] iperf network testing tool. Webpage. http://sourceforge.net/projects/iperf.

[7] tcpdump packet analyzer. Webpage. http://www.tcpdump.org.

[8] John Stratigakis. Hardware assist system and method for the timing of packets in a wireless network. US Patent 7233588, US Patent Office, June 2007.

[9] Stefan Kremser. Deauthentication and other wifi hacks. Webpage. https://spacehuhn.io

[10] Kody Bryan. Scan, Fake & Attack Wi-Fi Networks with the ESP8266-Based WiFi Deauther. Webpage. https://null-byte.wonderhowto.com/

[11]] Aircrack-ng, http://www.aircrack-ng.org

[12] Wireshark, http://www.wireshark.org

# THANK YOU