PROJECT TITLE

Submitted in partial fulfillment of the requirements

of the degree of

Bachelor of Engineering

by

KULJEET BHENGURA-05

KEVIN DSOUZA-17

DISHA SANIL-64

Supervisor:

PRASAD PADALKAR

Department of Information Technology

Don Bosco Institute of Technology

2019-2020

AFFILIATED TO

UNIVERSITY OF MUMBAI

DON BOSCO INSTITUTE OF TECHNOLOGY

Vidyavihar Station Road, Mumbai - 400070

Department of Information Technology

CERTIFICATE

This is to certify that the project entitled **"**Wifi Deauthenticator and Deauth Detector **"**is a bonafide work of

Kuljeet Bhengura	**05**
Kevin Dsouza	**17**
Disha Sanil	**64**

submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of **Undergraduate** in **Bachelor of Information Technology**

Date: 21/08/19

(Prof. Prasad Padalkar)
Supervisor

(Prof. Prasad Padalkar)
HOD, IT Department

(Dr. Prasanna Nambiar)
Principal

DON BOSCO INSTITUTE OF TECHNOLOGY

Vidyavihar Station Road, Mumbai - 400070

Department of Information Technology

Project Report Approval for B.E.

This project report entitled **"Wifi Deauthenticator and Deauth Detector"** by **TEAM 17** is approved for the degree of **Bachelor of Engineering in Information Technology**

(Examiner's Name and Signature)

1. ——————————————

2. ——————————————

(Supervisor's Name and Signature)

1. ——————————————

(Chairman)

1. ——————————————

Date: 21/08/19

Place: Mumbai

DON BOSCO INSTITUTE OF TECHNOLOGY

Vidyavihar Station Road, Mumbai - 400070

Department of Information Technology

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea / data / fact / source in my submission. I under- stand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

(————————————-)
(Signature)

(————————————-)
(Name of Student and Roll No.)

(————————————-)
(Signature)

(————————————-)
(Name of Student and Roll No.)

(————————————-)
(Signature)

(————————————-)
(Name of Student and Roll No.)

Date:21/08/19

ABSTRACT

Wireless networks are unlike wired when it comes to security factor, they are considered fundamentally insecure due to its nature of transmitting the data via radio waves and also the security design of WLAN structure exposed the medium to versatile attacks. This project sheds the light particularly on the availability factor, in which the attacker tends to exploit certain design flaws in wireless layer two (DLL Layer's MAC Layer) to disrupt the connection on the authenticated clients.
On the other-hand this paper discusses the possible ways to detect these types of attacks and how important is it to implement an automated method to detect these attacks.

The objective of this project is to investigate a special Denial of Service (DoS) attack against 802.11 wireless networks. This attack is known as the Deauthentication / Disassociation attack which is launched against 802.11-based wireless networks. When a client needs to disconnect from the wireless access point, it sends special frames known as deauthentication or disassociation frames. Due to being encrypted, these frames do not require an authenticated user. Hence, an attacker 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. In this project, an efficient solution is proposed to perform and prevent deauthentication attacks by verifying deauthentication frames.

Keywords: Wireless networks, WLAN structure, MAC Layer, ESP8266, Deauthentication/Disassociation, IEEE 802.11, access-point

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Problem Statement

Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Security is one of important challenge which is to be handled in the era of wireless technology these days. Current security standards have shown that security is not keeping up with the growing use of wireless technology. There are many security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Every now and then a new vulnerability comes in existence to the existing wireless standards. Our objective is to investigate and perform a special type Denial of Service (DoS) attack against a vulnerability in 802.11 wireless networks. This attack is known as the Deauthentication Attack. When any wireless access point wants to disconnect a client or terminate all the connections, 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. Along with the offence we also present an efficient defence 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 offence and defence strategy.

1.2 Scope of the Project

1.2.1 Scope of Offence

One place where Deauthentication can be particularly useful is at Schools or University. By blocking cell-phone Wi-Fi Hotspots, students can be prevented by being distracted on their phones. In addition, they cannot cheat by sending text messages to one another during exams. High security premises, such as prisons and detention centers, can also benefits from our module because it can prevent illicit communication between inmates and visitors.
Military Services: Prevent terrorist attacks by means of remote-controlled bombs. Any bombs can be disconnected from the master device using this Deauther.
Meetings: Help achieve quietness and silence in a conference room during a meeting.

1.2.2 Scope of Defence

1) 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.

2) Create awareness about 802.11w. The “w” protocol uses CCMP from 802.11i to provide integrity, confidentiality and sender authenticity for unicast management frames, and Broadcast Integrity Protocol (BIP) to provide integrity for broadcast management frames. In both cases, protection is only provided for management frames of subtype action, deauthentication and disassociation. If protection of management frames is enabled and an unprotected management frame of subtype action, deauthentication or disassociation is received, the frame is silently discarded.

1.3 Current Scenario

1.4

1.5 Need of the Proposed System

Wireless 802.11 standard [1] was founded to help people connecting more easily to networks and
internet. However, this medium suffers from several security concerns in terms of confidentiality,
integrity and availability. The 802.11 Wi-Fi protocol contains a deauthentication feature. It is utilized to detach customers from network. An attacker can send a station a deauthentication frame at any time, with a spoofed source address for the wireless access point. The protocol does not require any encryption for this frame, even when the session was established with. In order to overcome those concerns encryption algorithms like WEP and WPA come across to mitigate both confidentiality and integrity by adding additional security layer to wireless medium. These two encryption algorithms would encrypt network traffic when implemented successfully [1] [2]. An interceptor will be incapable to connect to an encrypted network nor to read or change the exchanged data. Unfortunately, WLAN developers have neglected the availability factor and left it exposed to different types of denial of service attacks. WLAN 802.11 frames consist of three major frames management, control and data frames [3] Data frame is whereas encryption applied. On the other side, both frames (Management and control) are responsible for power saving, association, deauthentication, disassociation, and authentication between the access point and the clients [4]. The absence of encryption implementation at both of management and control frames exposes the medium to persistent diverse types of DOS attacks at Data Link OSI Layer [3][4].The attacker might simply spoof the unencrypted Deauthentication/Disassociation message with the MAC address of particular access point and keep retransmitting it to all clients continuously causing a disconnection state in WLAN networks. Wireless Availability attacks can be classified according to each OSI layer with its risk level as depicted underneath in figure 1. This paper only focuses on MAC layer attack whereas the attacker is not conditionally connected to the network in order to launch an attack. The reason behind focusing on this layer is the shortage of concurrent solutions that mitigate Dos attacks on this particular level [5]. Different hard work and researches were performed to mitigate the attacks on application, transport and network layers yet unfortunately both layer two and one were neglected and left to be exploited by malicious

hackers.[3]-[4]-[5]

Deauthentication/Disassociation attacks are both parts from layer two, [5] however detecting these types of attacks requires a skillful network administrator therefore, the need for an automated monitoring tool raised to provide an easy way to alert the regular user if there is an aired Deauthentication/Disassociation attacks. The attacker tends to launch continuous flood of either deauthentication or disassociation for the sake of divulging hidden SSID of the targeted access point also to obtain a handshake to be used later on in cracking WPA2 encryption. [3] Another reasonable justification for the attack is to prevent the user to connect to the legitimate access point and to trap the clients to connect to rogue access point in order to steal, redirect or tamper client's data while en-route.

Target:

2. Wireless MAC Layer Attack Types

1. *Association/Authentication flood attack:*

In this state, the attacker spoofs source MAC addresses in an attempt to authenticate and associate to a particular access point. The attacker continually sends floods of either association or authentication requests, to fully consume the memory and processing capacity of targeted access point, leaving connected clients with either limited or no connectivity connection status.

2) Deauthentication/Disassociation flood attack:

Wireless Network is susceptible to Denial of Service Attack "DOS Attack" by means the attacker can use a spoofed deauthentication command to force the access point to re-authenticate the connected clients unfortunately this kind of attacks is considered unstoppable till this day in (a, b, g, n) standards. However, the new standards (ac) offers a partly protection against this attack only when encryption is implemented.

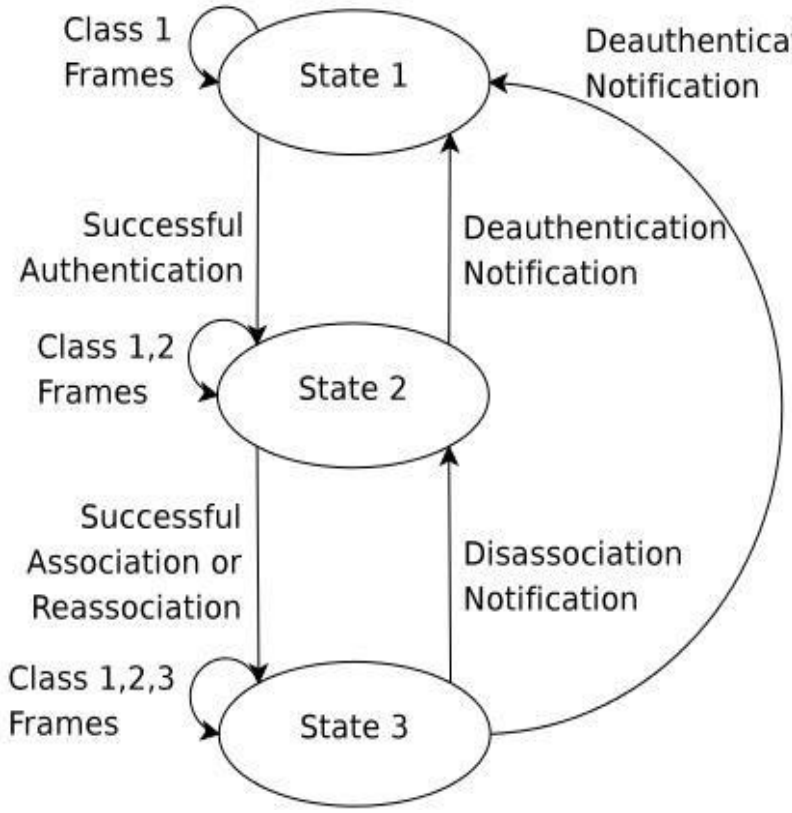


Fig 1.4.1: Process of Client-AP Authentication

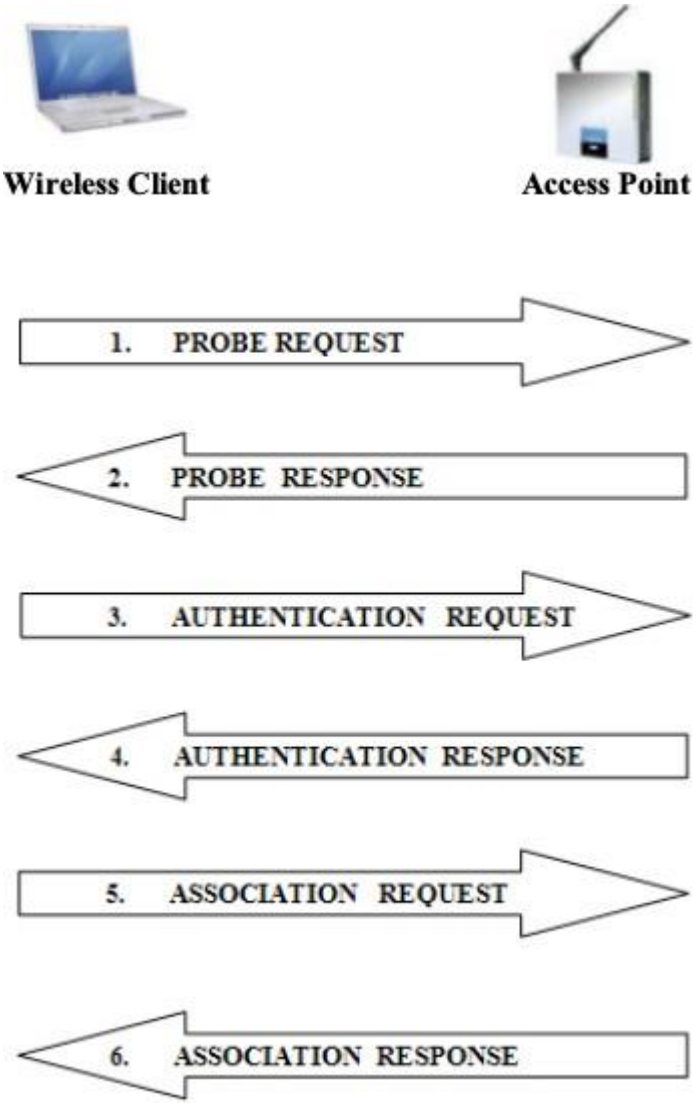


Fig 1.4.1 Two-Way Authentication

Chapter 2

Review of Literature

2.1 Summary of the investigation in the published papers

Definition: A literature review or narrative review is a type of review article. A literature review is a scholarly paper, which includes the current knowledge including substantive findings, as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources, and do not report new or original experimental work.

A literature review may consist of simply a summary of key sources, but in the social sciences, a literature review usually has an organizational pattern and combines both summary and synthesis, often within specific conceptual categories. A summary is a recap of the important information of the source, but a synthesis is a reorganization, or a reshuffling of that information in a way that informs how you are planning to investigate a research problem. The analytical features of a literature review might:

- Give a new interpretation of old material or combine new with old interpretations,
- Trace the intellectual progression of the field, including major debates,
- Depending on the situation, evaluate the sources and advise the reader on the most pertinent or relevant research, or
- Usually in the conclusion of a literature review, identify where gaps exist in how a problem has been researched to date.

2.1.1 Existing Attacking Systems

Before we can finally dive into our survey of Wi-Fi Deauthentication and Deauthentication Detector approaches per se, we must take a moment to make a few much-needed clarifications.

i) **Clarification 1**: Our goal in this section is to introduce, organize and review the existing systems similar to our systems, rather than to detail the exact algorithms that those systems employ. This is because common trends in the algorithmics of the reviewed solutions are currently rather limited across different sensing modalities.

ii) **Clarification 2**: The second clarification we must make is that since the authors of the solutions reviewed in this section often do not agree on common performance metrics or even experimental scenarios, we are forced to compare different approaches in rather qualitative terms. Thus, we use words such as “accuracy” and “precision” loosely to denote a measure of the average error and a measure of classification correctness.

A. Masquerading Attacks

In masquerading attacks, an attacker spoofs the MAC address of a specific station or AP. Due to the open nature of the wireless medium, an attacker can easily sniff wireless traffic in order to find the identities of the devices on the network. Those identities can then be easily spoofed by using device driver software. Below is a list of the attacks discussed in the literature until now.

1) Signal Jamming

The most basic form of DoS attack is when another signal interferes with data transmissions as shown in Figure 2.1 (reproduced from Codenotti *et al.* [10]). Such interference can occur continuously or intermittently and arise from a variety of sources apart from malicious activity.

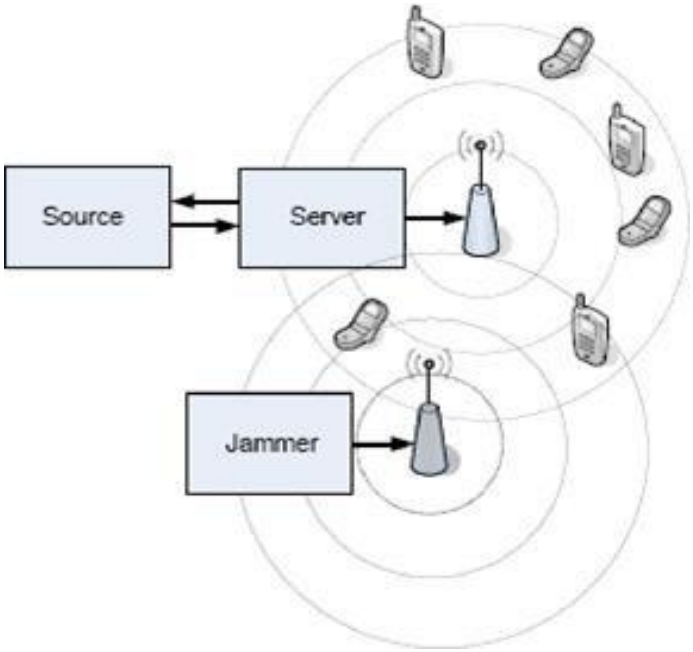


Fig 2.1.1 Signal Jamming Attack

2) Disassociation Attack

A very similar vulnerability may be found in the association protocol that follows authentication. The IEEE802.11 standard allows clients to associate with only one AP at a time. Similarly, to the authentication process, the IEEE 802.11 standard allows clients and AP to explicitly request disassociation from each other. As with authentication, association management frames are also unauthenticated. Exploiting this vulnerability is functionally identical to the deauthentication attack. However, it is worth noting here that deauthentication attacks are more severe than disassociation as they can cause stations to lose more time re-associating with the AP [5].

3) Power Saving attacks

In order to conserve power, the IEEE 802.11 clients can enter a sleep mode during which they are unable to transmit or receive. During this time the AP buffers all inbound data for the sleeping node until the client polls the AP for its data. By spoofing the polling message on behalf of the client, an attacker can cause the access point to discard the client's packets while it is asleep.

Along with spoofing polling messages, clients can also be tricked by spoofing the TIM to convince the client that there is no pending data present at the AP. Another vulnerability that arises from a power saving mechanism is due to the unauthenticated management frames used for synchronization purposes, such as TIM intervals or timestamp broadcasts. By forging these management frames, an attacker can cause a client node to fall out of sync with the AP and fail to wake up at the appropriate times [5].

4) 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 [14]. Using both narrow-band and wide-band jamming signals they report the results of jamming against a simple two station ad hoc wireless network. The results show that the encoding and modulation schemes have different characteristics:

- Direct-Sequence Spread Spectrum (DSSS) signals, as used in IEEE 802.11b, appear to be resistant to wide-band jamming. DSSS can continue to be work in the presence of a strong jamming signal by lowering the data rate.
- Orthogonal Frequency Division Multiplexing (OFDM) signals, as used by IEEE 802.11a and 802.11g are resistant to narrow-band jamming whereas it is vulnerable to a complete breakdown in the presence of a wide-band jamming signal.

IEEE 802.11 equipment is usually capable of operating in both DSSS and OFDM modes and so it's possible to minimise interference (whether unintentional or deliberately caused) by changing the data rate and/or transmission mode. In many commodity WNICs this can be achieved on frame-by-frame basis and allows for an adaptive defence to simple jamming strategies.

5) MAC-Layer Misbehaviour

MAC layer misbehaviour or cheating is a mechanism by which an adversary subverts the MAC-layer protocol to gain privileged access to the channel. The reason maybe simply to prioritise traffic or it could be used in conjunction with a traffic-flooding attack. In an IEEE
802.11 network node could reduce the size of the contention window or the back-off timers to gain access to the medium earlier than would normally be the case. Kyasanur and Vaidya studied the problem of misbehaving stations and proposed a mechanism for detecting such misbehaviour and changes to the MAC to enforce correct behaviour [32]. Although effective in the limited case this scheme assumes that the station is behaving rationally and is trying to maximise its own bandwidth for other purposes. The scheme does not stand up to a malicious adversary who is seeking purely to deny or degrade service. Cheating can also be detected in other ways. Raya et al. propose the DOMINO system which promiscuously monitors the network and identifies misbehaving stations [33]. This scheme is proposed for infrastructure networks and so DOMINO is either installed at the access point or runs on a monitor co-located with the access point. Since all stations communicate via the access point then any station not obeying the protocol's minimum inter-frame spacing is clearly cheating. What is more difficult to spot is a station which is using a non-standard contention procedure and picking slots early in the contention window. To make detection easier Raya et al. propose a protocol modification in which the receiver specifies the back-off times to be used by the sender. If the sender is observed to send before this time they can be presumed to be cheating.

Djahel and Naït-Abdesselam propose a similar scheme for MANETs (and, by extension, WMNs) that also modifies the protocol to make detection of cheating stations easier [34]. In a

MANET environment there is no centralized monitor and so the receiver and neighbours are responsible for detection of any misbehaviour on the part of the sender. The scheme modifies the RTS frame to make detection of cheating possible by other stations and this allows a receiving station to withhold the CTS from stations which appear to be cheating. Bansal

also try to resolve the problem of detecting misbehaviour but this time in WMNs using a simple statistical model and employing simple cut-off values to detect cheaters [35]. Their work is conducted in a real mesh network as opposed to a simulation and so modification of the MAC protocol is much more difficult but the detection model is far from satisfactory.

A key problem when detecting misbehaviour between neighbours is not always apparent in the simulation-based studies cited above. This is that a node may monitor neighbours which are out of radio range of each other as shown in Figure 2.2. In this case neighbour A may not hear a transmission from neighbour B and could legitimately broadcast during B's DIFS period. The use of RTS/CTS cannot eliminate this problem and the monitor must have some way of knowing which neighbours are actually in range of each other to disambiguate between cheaters and legitimate stations. This information may be available directly from the routing protocol or it might be necessary to implement a protocol such as the Neighbourhood Discovery Protocol (NHDP) [36] to discover the topology of the local network neighbourhood.

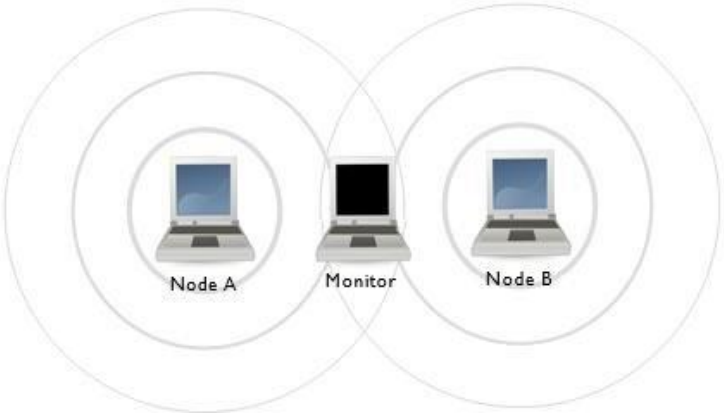


Fig 2.1.2 MAC Layer Misbehaviour

5) Traffic Flooding

Traffic flooding is a well-established technique in wired networks for consuming bandwidth. By flooding the network with traffic, or otherwise causing network congestion, authorized stations will not be able to make use of the bandwidth. Traffic flooding in wireless LANs exploits the inherent unfairness present in the MAC layers of many wireless network de- signs. Contention based access schemes often permit channel capture by stations because:

a. Exponential back-off favours stations which have already gained access to the channel

b. Stations that generate the strongest signals will capture the channel despite the RTS/CTS handshake. Ware et al. experimentally validated this behaviour [30], re- futing the claims of a number of simulations.

c. Stations can cheat at the MAC layer to increase their chance of channel capture

Gupta et al. demonstrated that in the face of such attacks the approaches used in wired networks for detection and prevention are ineffective [31]. They propose a fair MAC as the solution to these problems which has the benefit of also addressing the problem of misbehaving stations (those not obeying the MAC to obtain more bandwidth). IEEE 802.11- 2007 does not provide a fair MAC but does define several Coordination Functions (CFs) to provide contention-based and contention-free access to the wireless channel. The contention- based mechanisms use an exponential back-off which favours stations that are placing the network under heavy load. This inherent unfairness is exploited by traffic- flooding attacks to deliberately starve other stations of bandwidth.

2.1.2 Different Methods to Prevent Attacks on Wi-Fi

Throughout this section a series of DoS vulnerabilities have been presented and the appropriate solutions described. These have been intended to illustrate the argument that there is no single threat to and no single mechanism can guarantee availability. Nevertheless, once a DoS attack is detected it is possible to employ countermeasures that apply to a variety of different attack types.

1. Baber Aslam et al. [12]

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.

2. Jing-Wei Zhou and Sheng-Ju Sang [17]

This paper shows 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). It also talks a little about EAP-MD5, EAP-TLS and EAP-TTLS. But its main concern on PEAP how its authentication process take place what are the defects in EAP-PEAP and how we can improve PEAP so it can overcome through these defects.

3. Swati Sukhija and Shilpi Gupta [31]

This paper dealt with description different protocols for securing Wireless-LAN. WEP is not able to provide security against various attacks and threats. Then WPA was come into picture which is a temporary solution to the security faults identified in WEP. But it is still prone to

various attacks like Beck-Tews, Chop-Chop etc. Thus, WPA2 was introduced providing an enhancement over WPA. WPA2 provide strong encryption by using block cipher AES but it is still vulnerable to attack due to sharing of GTK among clients and transmission of unencrypted control and management frames. Also, WPA2 does not support legacy hardware unlike

4. Static 4-Way Handshake

Floriano De Rango et. Al., [14] proposed static dynamic 4-way handshake solutions solutions to avoid denial of service attack in WPA and IEEE 802.11i. Paper also explained DOS and DOS Flooding attacks against IEEE 802.11i 4-way handshake. Paper also compared static versus dynamic resource-oriented solutions for the 4-way handshake.

5. Arash Habibi Lashkari, *et al.*, [8]

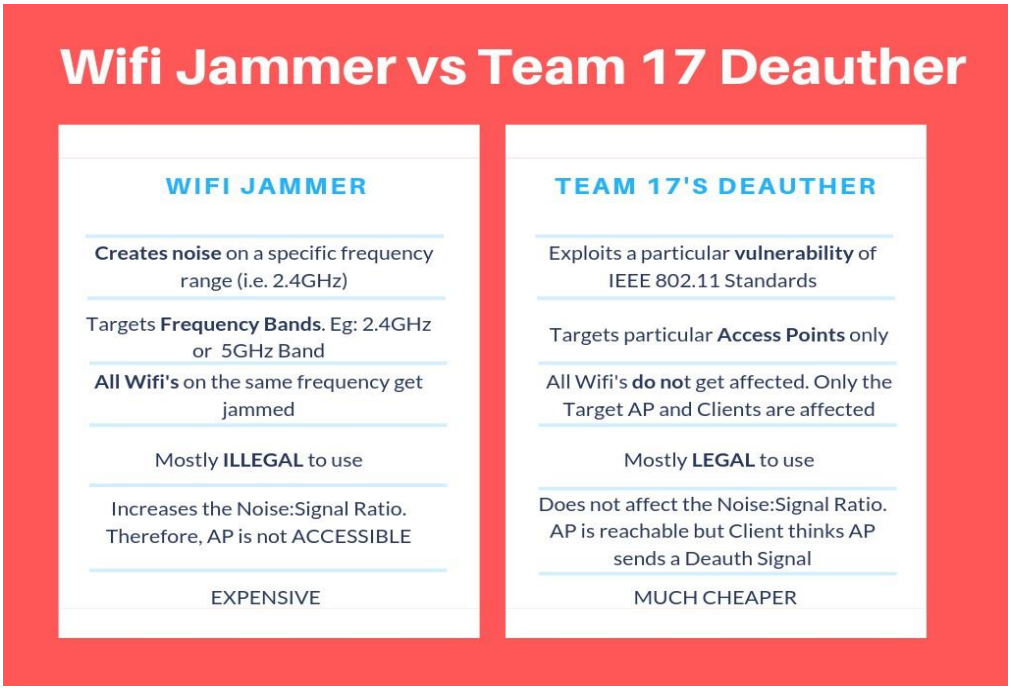
This study presented a survey on wireless security protocols (WEP, WPA and WPA2/802.11i). Here WEP protocol types, weaknesses and enhancements, WPA protocol types, WPA improvements such as cryptographic message integrity code or MIC, new IV sequencing discipline, per packet key mixing function and rekeying mechanism. They also explained major problems on WPA that happened on PSK part of algorithm. Finally, paper explained third generation of wireless security protocol as WPA2/802.11i.

2.2 Comparison between the Tools/ Methods / Algorithms

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

Table 2.2.1 Types of DOS Attacks and Countermeasures



2.2.2 Difference between Wi-Fi Jammer and Team17 Deauther

2.3 Algorithm(s) with example

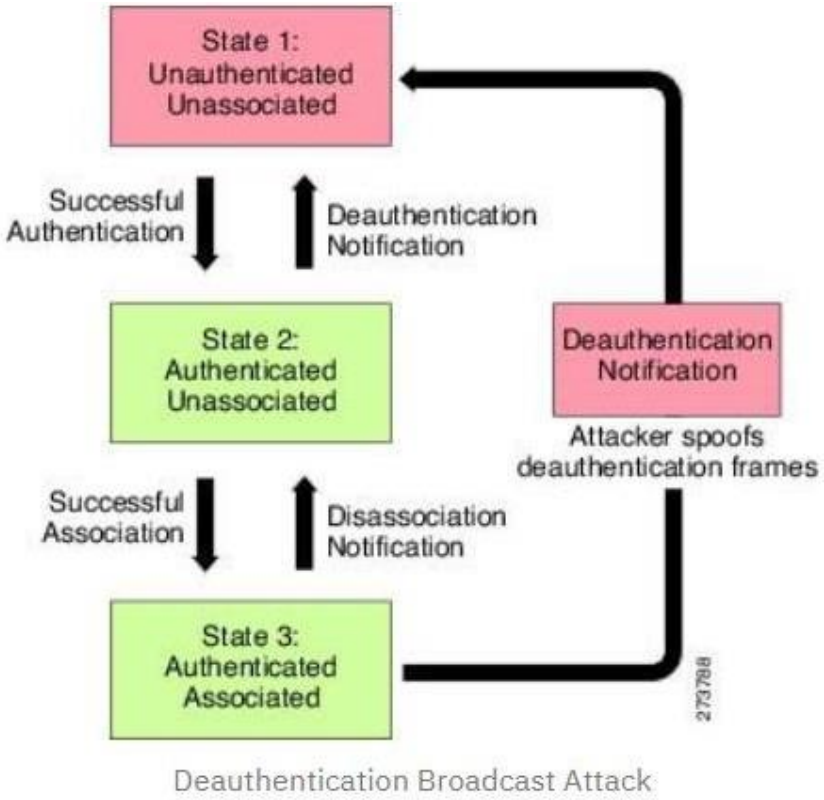


Fig 2.3.1 Steps performed in Deauthentication

STEPS PERFORMED BY THE DEAUTHENTICATOR:

STEP 1: Get Your Board Ready

STEP 2: Look for the Control Access Point

STEP 3: Perform a Scan of the Area

STEP 4: Select Target Networks

STEP 5: Launch an Attack

STEP 6: Customize Your Settings

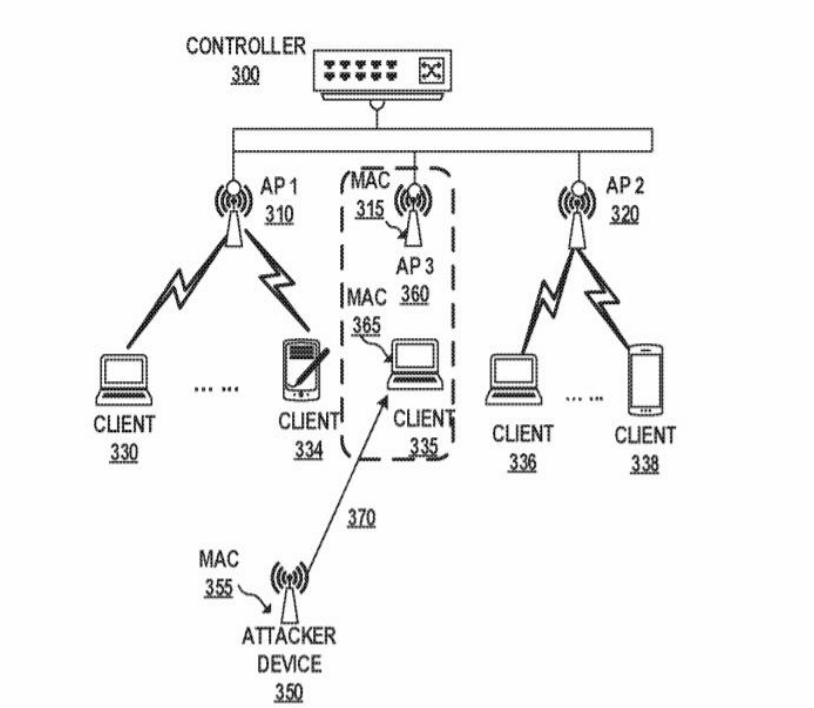


Fig 2.3.2 Steps performed in Deauth Detection

STEPS PERFORMED IN DEAUTHENTICATION DETECTOR:

STEP1: Turn on the Detector. We can define whether or not we want to Channel Hop or just stay on one channel by setting the "ChannelHopping" setting to "true."

STEP 2: Next, we have a series of variables which keep track of things in the script. We have added two variables to keep track of deauthentication and disassociation packets, creatively named "dissoc" and "deauth."

STEP 3: Next, we have a sniffer function to track the packets individually.

STEP 4: Instead, we'll insert two "if" statements that will add to a cooldown timer.

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

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

STEP 5: Now, our module decides what happens when the packet doesn't match, meaning it's a normal Wi-Fi packet. If Deauthorisation packet then LED is turned on and if normal packet then LED turns off after 12 seconds(approx.) from the last detected Deauthorisation packet.

Chapter 3

Analysis and Design

3.1 Methodology / Procedure adopted

Describe on the development methodology / model you would use. (E.g. Agile method or Iterative Model)
How you intend manage the weekly meetings?
How do you intend to monitor and measure the progress of the project?

3.2 Analysis

Based on the requirements gathered, how was the feasibility study of the project carried out?
If any requirements, were modified why they were modified?

3.2.1 Software / System Requirement Specification - IEEE format

3.3 Proposed System

Give the details of your proposed system and architecture Advantage of the proposed system over the existing system

3.3.1 Hardware / Software requirements

Development Hardware / Software requirements
Deployment Hardware / Software requirements

3.3.2 Design Details

Different UML diagrams as per the project requirement (For e.g. Use Case Diagram)

3.3.3 Implementation Plan

Timeline chart is for Next semester

Chapter 4

Results and Discussion

This chapter would contain the summary of proposed system / algorithm

Also this would contain the task completed and the contribution of team members.

Chapter 5

Conclusion

Summary of the entire report

Appendix - I

Data Sheet(s) - Electronic component

Installation Procedure - Development Software

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

[13]S. D. Kanawat and P. S. Parihar, Editors, "Attacks in Wireless Networks", International Journal of Smart Sensors and Adhoc Networks, (2011) May 18-23.

[14] Y. X. Lim and T. Schmoyer, Editors, "Wireless Intrusion detection and response", IEEE Information Assurance Workshop, (2003) June 18-20, Westpoint, Newyork.

[15] K. Bhatele, A. Sinhal and M. Pathak, Editors, "A Novel Approach to the Design of New Hybrid Security Protocol Architecture", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), (2012) August 23-25, Ramanathapuram