Fall 2011

Scanned Wireless Network Setup Fake Access Point & its Detection

Saurabh Vishal
San Jose State University

Follow this and additional works at: https://scholarworks.sjsu.edu/etd_projects

Part of the [Computer Sciences Commons](#)

Recommended Citation

Vishal, Saurabh, "Scanned Wireless Network Setup Fake Access Point & its Detection" (2011). *Master's Projects*. 209.

DOI: <https://doi.org/10.31979/etd.x928-hf83>

https://scholarworks.sjsu.edu/etd_projects/209

This Master's Project is brought to you for free and open access by the Master's Theses and Graduate Research at SJSU ScholarWorks. It has been accepted for inclusion in Master's Projects by an authorized administrator of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.

Scanned Wireless Network Setup Fake Access Point & its Detection

A Writing Project

Presented to

The Faculty of the Department of Computer Science

San José State University

In Partial Fulfillment

of the Requirement for the Degree

Master of Science

by

Saurabh Vishal

Summer 2011

Copyright © 2011

Saurabh Vishal

ALL RIGHT RESERVED

SAN JOSÉ STATE UNIVERSITY

The Undersigned Project Committee Approves the Project Titled
Scanned Wireless Network, Setup Fake Access Point and its Detection

by

Saurabh Vishal

APPROVED FOR THE DEPARTMENT OF COMPUTER SCIENCE

Dr. Soon Tee Teoh	Department of Computer Science	Date
-------------------	--------------------------------	------

Dr. Robert Chun	Department of Computer Science	Date
-----------------	--------------------------------	------

Mr. Akhil Kapoor	Ebay, Senior Software Engineer	Date
------------------	--------------------------------	------

Abstract

This thesis addresses the topic of development and advancement of the wireless technology. Report described about network monitoring and security issues with advancement in the increase of network bandwidth and user requirements to access the internet. This report mainly focuses on how war driving affects the security of end user. How it can solve problem for infected users who are accessing the internet.

The technique is used in wireless environment where all kinds of wireless devices can access internet and can use network resources with high security and better performance.

Research on this topic reveals that passive monitoring technique can be used to scan the wireless network without even letting other devices to know that scanning is going on. In this way air traffic can easily be sniffed, which raises many security risks and threats related to sniffing the air traffic in wireless network that can easily reveal the personal identity of the end user who is using the wireless network. I have considered Man-in-the-middle scenario to implement FakeAP where the end user has to compromise its security in order to gain access to the network resources. I have also developed a solution to detect the FakeAP in the network which is misusing the network resources and wrote a program to trace down its location on Google maps.

Table of Contents

List of Figures (continue numbering sequentially)	3
List of codes (continue numbering sequentially)	4
List of Tables (continue numbering sequentially)	5
Acknowledgements	6
1. Introduction	7
1.1 Purpose and Scope	8
1.2 Motivation	8
2. Wireless Network	11
2.1 Types of Wireless Network	11
2.2 Wireless LAN	11
2.3 Wireless Architecture	12
2.4 How WLAN Works?	14
3. Wireless 802.11 Security Standards and Protocols	16
3.1 802.11 Frame format	16
3.2 EAP methods	18
3.3 WEP (Wired Equivalent protocol)	19
3.3.1 How WEP authentication works?	20
3.3.2 RC4 encryption algorithm	21
3.4 WPA (Wi-Fi Protected Access)	23
3.4.1 TKIP (temporal key Integrity protocol)	23
3.4.2 How does TKIP works?	24
3.4.3 MIC (Message Integrity code)	25
3.5 WPA2	26
3.6 MAC PDU	27
4. Wireless Security threats and Vulnerabilities	29
4.1 Man in Middle Attack	31
4.1.1 Eavesdropping	32
4.1.2 Manipulation	32
5. Project overview	34
5.1 Passive Scanning approach	34
5.2 Algorithm overview	35
5.3 Pseudo code	36
5.4 Flow Diagram	37
5.5 Track down Location	38
6. Implementation Environment	39
6.1 Hardware Requirements	39
6.2 Software Requirements	39
6.2.1 Python 2.6	39
6.2.2 Scapy 2.1	40
6.2.3 Scapy Dependencies	41
6.2.4 Django Framework	42
6.3 Implementation code	43

7.	Testing Environment.....	50
7.1	Metasploit Framework.....	50
7.2	Fake Access Point Module	50
7.3	Dependencies.....	52
7.4	DHCP server configuration file.....	52
8.	Conclusions & Future Work	60
	ACROYNMS.....	62
	REFERENCES.....	63

List of Figures (continue numbering sequentially)

Figure 2.1 Wireless Local area network	12
Figure 3 (a) 802.11 Format	17
Figure 3.3 WEP (Wired Equivalent Protocol)	20
Figure 3.4.2 : TKIP Protocol	23
Figure 3.4.3 : How TKIP works	25
Figure 3.5 MAC Data unit format	27
Figure 5: Wireless Scenario	34
Figure 5.4 Flow chart for detection algorithm	37
Figure 6.2.2 Scapy Mechanism	41
Figure 7.4 dhcp.conf File	53
Figure 1.The terminal output of the scanned wireless access point.	54
Figure 2.Start Django server with (python manage.py runserver)	55
Figure 3.Find Access point on Network	55
Figure 4.List of available wireless access point nearby region	56
Figure 5.Setting Up the fake access point using shell script	56
Figure 6.You can see “ freeSJSU” access point is highlighted in windows.	57
Figure 7.Connect the client terminal “windows” to “freeSJSU” Fake connection	57
Figure 8.Once connected if client want to get access to the internet from this connection. This screen will appear on his browser.	58
Figure 9.On Linux terminal we can see the connection established and what client want to access on the web browser.	58
Figure 10.Fake access point is detected while connection is established on the machine.	59
Figure 11.We can track down the location of machine using google API	59

List of codes (continue numbering sequentially)

Code 3.3.3 (a) Key Scheduling Algorithm	22
Code 3.3.3 (b) RC4 Algorithm	22
Code 5.3 Fake AP detection Algorithm	36
Code :6.3 (a) urls.py	43
Code: 6.3 (b) view.py	44
Code: 6.3 (c) Scan_wifi.py	46
Code:6.3 (d) Fake AP detection.py	47
Code: 6.3 (e) location.py	49
Code7.2 (a) New access Point Interface Module	51
Code 7.2 (b) Starting Access Point module	51

List of Tables (continue numbering sequentially)

Table 3 (i) Security standards of 802.11 IEEE

16

Acknowledgements

This study would never have been possible without the guidance and help of several individuals who in one way or the other contributed and extended their valuable assistance in the preparation and completion of this project.

The First and the my foremost gratitude is to Dr. Soon See Teoh who has helped me in assisting to complete this work and to my committee members Dr. Robert Chun and Mr. Akhil Kapoor who supported me in my work to finish it on time.

Last but not the least my family and my friend who constantly supported me.

1. Introduction

Today the Internet has become essential requirement for everyone, whosoever wants to remain connected with the world. Mobile devices and wireless laptops have changed our working style and mannerism. The online market has been growing whether it is in the field of communications, E-commerce, Banking or retail. The end users are very frequently using the internet and using their private identity online, by sharing their data on the internet which can be easily sniffed from the air by using some tools that are available today. Here comes the hard part of using wireless devices in the network, as everyone is using mobile phones, wireless laptops which contain the WLAN card to connect to the access point in the wireless local area network [20]. The wireless network is one of the most enhanced sectors because of its flexibility and mobility; it is used in every sphere of communications nowadays like business, education or research, so it has become an integral part of life. This technology have certain disadvantages also; there are ways by which air traffic can be sniffed using network interface card in monitor or RFMON mode [16]. Today every Wireless LAN card used in laptops has a monitor mode and that can be enabled by using different open source tools that are available in the market. Which can be installed on the laptops and wireless air traffic can be sniffed very easily. Some software like Netstumbler for Windows and Kismet for Linux are used to capture the air traffic of the wireless LAN.

Here, I have explained a simple example of DOS attack where a legitimate user want to gain access to website on internet but someone is performing denial of service attack on the server side or on his machine due to which end user is unable to get access

to the website. There are certain measures one should follow to reduce the possibilities of wireless attacks such as disabling its SSID broadcasting, changing the default SSID and changing encryption mode to WEP (wired equivalent privacy) to WPA2 [19].

1.1 Purpose and Scope

The purpose of the tool I have developed is to find out the security vulnerabilities in the wireless network and other network management faults. To determine how many access points are available in wireless LAN and where they are installed. To track down its location and to check whether they are properly configured or not, what are their configuration settings and on which firmware they are working with their vendor specifications. What security measures should end user must follow to avoid these weaknesses and how can it be solved? I have mainly focused on monitoring the wireless LAN that should be done periodically as access points can be change their position from one network to another frequently because of the mobility of the wireless devices to move in the network. The tool should be able to check the signal strength of the wireless network so that thorough checking should be carried out when required. The approach I followed in capturing 802.11 packet using tool like scapy which works with low level libraries like pcap and wincap of airdump.

1.2 Motivation

The motivation to work on this project comes from security issues and attacks that are present with related security risks associated in wireless network. Today in the market there are many war driving tools that are available and used to capture the air traffic. Attackers can use these tools to capture the end users information that can

reveal its personal identity and other valuable information. There are security standards that are defined in IEEE for 802.11 protocols. Still there are some attacks that can easily rule out the security of home network as well as enterprise network. Linux, which is powerful operating system, supports lot of open source tools that can be used to break the security. So the question is: How can we detect when one has become the victim of the attacker.

I have designed a system which can help the end users to detect the FakeAP on their network and get rid of it. The system works on the principle of LSF (Least Square fitting method). I have used python language and scapy tool to scan the wireless network using passive approach and gathered the information needed from nearby wireless access point available in the network. The information like its SSID, BSSID, Encryption mode and channel of the required AP is gathered to find out the “timeval” field of each access point from its 802.11 beacon frames and calculates the “clock skew” of each AP. Once that “clock skew” is measured and stored. It is used to check the “timeval” field in next scanning interval again to check whether the AP is Fake or not. The threshold value has to remain fixed once it is calculated. It works on the principle of difference between clock skew. If ‘timeval’ field of same AP has a difference in clock skew and difference is bigger than the threshold then it’s a FakeAP.

This project deals with handling the FakeAP on wireless network. I have also tested my approach by creating and installing a FakeAP on a Linux machine that uses various open source tools like Metasploit framework with aircrack-ng package which

is used to sniff the air traffic using pcap libraries in Linux environment. For installing a FakeAP on the network, DHCP server should be configured on the machine, it is used to forward the packet request to the client once IP address has been assigned to client machine.

The end user can track the location of the FakeAP in the nearby wireless network where it has been installed and take required measures to get rid of it. The wireless risk has been increasing very frequently and personal identity of the users is at compromise, if they want to gain internet access. I have also mentioned some of the counter measures that the end users must follow once it is discovered that it is connected to FakeAP in the last section of the report.

2. Wireless Network

Wireless network can be defined as any type of computer network which is not connected through any kind of wire. The nodes in the network are connected by wireless medium like radio frequency waves and transmission usually takes place at layer 1 and layer 2 of the network [20][24].

2.1 Types of Wireless Network

There are many different wireless networks: They are Wireless Personal Area Network (WPAN), Wireless Metropolitan Area Networks (WMAN), mobile devices like GSM and Personal communication service (PCS) and Wireless Local Area Network (WLAN) [24]. This report mainly focuses on Wireless local area network. Most WLAN are IEEE 802.11 standard based technologies and Wi-Fi (Wireless-Fidelity) a technical certification of the interoperability between IEEE 802.11 devices, which is often referred to as IEEE 802.11[9].

2.2 Wireless LAN

Wireless LAN can be defined as network of wireless devices that are interlinked with each other by wireless medium. WLAN uses radio waves signals that work on spectrum mechanism technology with in limited area called as Basic service set (BSS). WLAN provides a major advantage over the wired network as the end users can move in an area and remain connected with the network. It provides mobility and scalability with broad range of coverage area. This advantage has made this

technology so popular among the end users that it is widely used in every field today [20][7][24].

Figure2.2 Wireless Local area network

2.3 Wireless Architecture

WLAN consists of various kinds of devices such as mobile phones, satellite hardware or GPS system , 802.11 router and network cards. Nowadays the laptops have in built wireless NIC card. All the devices in the wireless network are called stations. Each station has a Wi-Fi network card (WNICs). They fall into two categories: access points and clients. The BSS area covered by WLAN has an identifier called Service set identifier (SSID). Standards are defined in section 3 that are used in WLAN .The following components are used in wireless LAN for establishing a wireless connection [23][24].

- **Basic service set (BSS)** is referred to all the stations that can communicate with each other in wireless network. There are two kinds of BSS. One is Independent

BSS called as IBSS and the other is called as infrastructure BSS. It contains an identifier (ID) called BSSID, which is MAC address of the AP serving that BSS.

An IBSS is an ad-hoc network that has no access points, that means it cannot connect to other basic service set. Whereas in infrastructure mode, they can communicate with other stations not in same BSS via APs.

- **Access points** are the BS (Base Stations) by which clients perform communication with other clients in the network through radio frequencies. The access point provides data encryption standards using WEP and WPA to improve the security. It also has unique MAC address.
- **Clients** are devices that use resources of the WLAN. The devices in the network are connected to APs using Wi-Fi network interface card that has a unique MAC address. The devices generally used are mobiles, PDAs and laptops, etc.
- **Service set identifier** is of 32 bytes of length and name given to BSS. A single access point can serve more than one BSS; it can have more than one SSID in the wireless network.
- **Channel** is the transmission medium of radio frequency used by APs to transmit the data to the BS. There are 11 different channels available in RF mode from 1 to 11 channels. If same channel is used by another network in nearby area then it can cause interference and poor quality of communication.
- The access points in the wireless network can hide their SSID name. These APs are called as closed AP whereas the access points that broadcast their SSID are called as Open AP. The devices connect to AP with its SSID signal strength. In

case of closed SSID name, clients has to manually establish a connection with that particular SSID name. The WNIC card send connection request through all channels, an access point receives the request from the client and approves its connection.

2.4 How WLAN Works?

WLAN architecture defines the components of wireless network. To establish a connection between the devices there are generally five basic steps [7][8]:

First is Scanning, process for finding wireless network in nearby region, stations uses scanning module to find the existing networks in that area. For this procedure they have to consider certain parameters listed below:

Types of BSS whether it is Ad-hoc or Infrastructure Networks

- BSSID can be individual or broadcast. Access points can choose on which BSSID it will transmit. If AP uses individual BSSID, then it is invisible. Broadcasted SSID can see all stations in its range.
- SSID (Network Name) with scanning type whether it is using active or passive technique and channel list on specify on that channel clients want to setup connection with probe delay parameter
- The wireless medium of the radio frequency is used by a station in wireless LAN for communication. To keep track of the location of the access point and number of access points present in that area so that the network can deliver better performance and coverage. For covering the maximum area, the access point should be present in

the range of another access points. So they can provide better transmission rate and performance in communications and connectivity.

3. Wireless 802.11 Security Standards and Protocols

The 802.11 standards are defined on 2.4, 3.6 and 5GHZ of frequency band in air for use of wireless Local area network (WLAN). There are many air modulation techniques used in this protocol, but mainly 802.11g and 802.11b are used. The table below defines the specification of 802.11 standards [9].

802.11 network standards				
802.11 protocol	Frequency (Hz)	Bandwidth	Data rate per stream Mbits/sec	Range
a	5,3,7	20	6,9,12,18,24,36,48,54	35 m ,115 ft
b	2.4	20	5.5,11	38 m, 125 ft
g	2.4	20	6,9,12,18,24,36,48,54	38 m, 125 ft
n	2.4,5	20,40	15,30,45,60,90,120,135,150	70 m, 250 ft

Table 3 (i) Security standards of 802.11[9]

3.1 802.11 Frame format

The 802.11 defines fixed standards for frame types for use of data communications. Frames have different sub fields like MAC header, Payload and FCS (frame check sequence). The first 2 bytes of MAC header describes the form of frame control field that defines its function and specification for use. Further control field is divided into sub fields described below:

- **Protocol version:** - 2 bits are used to represent it and zero is assigned to default in current version

- **Type:** 2 bits are used to identify type of WLAN frame, control and data and to manage various frame types as defined in 802.11 standards.
- **Sub type:** Provides extra information about frames.
- **To DS and From DS:** Both use a single bit for identification whether data frame is headed towards Distributed system or not. In CMF (Control and management frames) values are set to zero. The bit is set for all the data frames. For infrastructure based networks this bit is always set to zero.
- **More Fragments:** this bit is set when frame is divided into multiple frames, except the last frame.
- **Retry:** this bit is set when retransmission is required to send the packet again.

802.11 FRAME FORMAT

Figure 3 (a) 802.11 Format

- **Power management:** Access point is required to manage power saver bit and connection.
- **More Data:** this bit is used by AP to activate stations in power saver mode.
- **WEP:** this bit is set whenever processing frame is modified, and it is changed when frame is decrypted. If there is no encryption it is always set to 1.
- **Order:** this bit is set when delivered method follows a strict order.

3.2 EAP methods

EAP is a single authentication method used in IEEE 802.11 standards. EAP stands for Extensible authentication protocol. It is a framework used in wireless networks and peer to peer networks that is defined as a standard in RFC3748, and further enhancement was done in RFC5247 [5].

The wireless networks use EAP method to generate a key and parameters required for authentication purpose. This method is not wired protocol; it defines the message format only [3]. There are different vendor specific methods that are defined in RFC's. The encapsulate messages are embedded within the protocol method.

For IEEE 802.11 protocol uses two methods of encryption: WPA and WPA2. These are official authentication mechanisms adopted by EAP protocol. The most commonly used methods are EAP-TLS, LEAP, EAP-AKA, EAP-SIM and EAP-TTLS [3]. These methods are described below:

- a) LEAP stands for (light weight extensible authentication protocol). It supports the repetitive authentication mechanism for clients and servers. It basically uses login password mechanism for authentication. LEAP frequently delivers session keys to authenticate wireless stations for encryption.
- b) EAP-TLS generally deals with transport layer security and was invented by Microsoft in PPP network. It is based on 802.1x/EAP architecture. The components in the 802.1X authentication process takes place basically at the end users or the client machine and AP working as an authenticator for the client, and network contains an

authentication server that deals with APs. The radius server is generally used to support EAP-TLS authentication.

c) EAP-AKA includes authentication and key management mechanisms that runs on symmetric cryptography that works on a challenge – response approach.

d) EAP-SIM is an authentication method that works on the subscriber identity module.

The EAP server is used as a backend authentication server using AAA protocol. It simply relies on EAP messages to and from server, and all the communication is performed by AAA protocol.

e) EAP-TTLS (Tunneled transport layer security) is a method that has made advancement over TLS but it does require each user to be issued a certificate, which the server uses for authentication. Password is used as the user authentication method. In this mechanism the passwords are transported in an encrypted manner within a high secure tunnel established based on server certificates.

3.3 WEP (Wired Equivalent protocol)

In wireless networks, WEP was initially used for a linked layer security option that was defined in 802.11 standards. WEP uses the RC4 encryption method with a 64 or 128 bit key to provide data packet encryption. As it provides the integrity and confidentiality equivalent to a wired network, every station in the wireless network must share the same secret key with the AP [19][23]. The key can be either a password or string of character that is shared between the devices in the network. The message is encrypted with 24 bit IV (initialization vector) during transmission.

Figure 3.3 WEP (Wired Equivalent Protocol)

The Plain text is mixed with data and encrypted with a CRC 32 bit per packet encryption key. Its main advantage is that it can reuse the IV with any frame.

3.3.1 How WEP authentication works?

The first step is to distribute the key in an out of band frequency, which is secured and encrypted [15]. The wireless stations share the secret key with the access point.

Then AP sends a Nounce (Challenge) to the work station to authenticate it.

In final step, the work station sends a response to the access point with the response containing the Nounce and the encrypted shared key between both.

In this way, authentication occurs in a wireless scenario between the AP and the clients in the network. More security can be provided by the enterprise that makes this technique more attractive. Access points can also be configured in bridge mode that connects wireless clients with an internal network. The AP should be allocated for remote management and SNMP (Simple network management protocol), which has dedicated IP address.

3.3.2 RC4 encryption algorithm

RC4 encryption and decryption is performed with the bitwise Exclusive-OR operation with the plain text. The algorithm generates key stream using a random number first and then generates the cipher, which includes the secret state that consists of two parts [22].

- A permutation of 256 bytes
- Two 8 bit index pointers

The key scheduling algorithm (KSA) is used to permute the combination with a variable key length. Once this operation is completed, the stream of bytes is generated using a pseudo-random generation algorithm (PRGA). Typically the key length is between 40 bits and 128 bits [15].

- a) **Key Scheduling algorithm** is used to initialize permutation in the array, and the keylength ranges between ($1 \leq \text{keylength} \leq 26$). Consider two 8 bit index registers as 'i' and 'j'. the pseudo code of KSA is given below

```
For i from 0 to 255
    Arr[i] = i;
Endfor

For (i from 0 to 255)
    J = (j + arr[i] + key [i mod keylength] mod 256
    Swap values (arr[i] and arr[j])
End for
```

Code 3.3.3 (a): Key Scheduling algorithm [24]

The RC4 algorithm is used to alter the state and output of each iteration in key stream. Here is pseudo code for this algorithm

```
i = 0
j = 0
While generating output:
    i = (i+1) mod 256
    j = (j+1) mod 256
    Swap values (S[i] and S[j])
    K = s[(s[i] + s[j]) mod 256]
    Output k
endwhile
```

Code 3.3.3 (b) RC4 Algorithm [24]

The plain text of 24 bit inserted in a random number generator and then output is Ex-ored with plain text, which is to be encrypted. The reverse procedure can be followed at the receiver end, but the condition is that the receiver should know the IV and key. So that it can decrypt the encrypted text.

3.4 WPA (Wi-Fi Protected Access)

WPA was released by Wi-Fi alliance as a security standard for Wireless Local area networks. It was developed to overcome the weakness of WEP encryptions and attacks that had been introduced. WPA consists of three basic components, which as a whole system provide this protected access for the end user. It works on 802.1X, TKIP and MIC.

3.4.1 TKIP (temporal key Integrity protocol)

TKIP was designed to preserve the compatibility between the existing infrastructure of the wireless LAN and the hardware used in WLAN so that WLAN can be easily upgraded. The main advancement that was done in this protocol was to generate a different key for every packet instead of using IV (Initialization vector) and concatenating with a shared key [16].

Figure 3.4.1: TKIP Protocol

In most devices in the wireless network, cryptographic functions are hard code in the wireless hardware. Therefore, there is problem in upgrading the firmware.

Upgrading can't be done very often as it is a costly and time consuming process. Because of this drawback, WPA protocol reuses some of the functionalities of WEP protocol of hard coded features to ensure compatibility and performance. The stream that is mainly used is RC4 i.e. hard coded in WNIC & it can't be changed. TKIP uses the RC4 again as a stream cipher, but it has changed the mode in which the secret key is shared. This made significant changes in wireless technology to establish security measures against any attacks. In session, a seed is provided for each packet key and then a session key is generated.

3.4.2 How does TKIP works?

In TKIP, a separate key is generated through a key function for each packet by hashing the MAC address of the sender machine with the initialization vector and session key for that particular session. The Key function is divided into two phases.

Phase1: Most processor intensive tasks are performed in this phase; the MAC address of the user machine with a temporary session key that is generated by the key function is hashed with 32 bits of the initialization vector. And the final result remains unaffected until and unless the session key is changed or the initialization vector of 32 bits is incremented.

Figure 3.4.2 How TKIP works

Phase2: The Receiver calculates each packet at the receiver end. The result of the phase1 and lowest 16 bits of each packet are hashed together, and the outcome is 104 bits per packet key.

After completion of both the phases the process of encryption is very similar to that performed for WEP, but the only difference is that WEP uses its lower 16 bits of Initialization vector with dummy values or some random bytes are injected in the middle of the key & then key function replaces the WEP key with per-packet key. Decryption should also be performed on the other end. TKIP improved the wireless security to a considerable amount with 128 bit dynamic key encryption. 24 bit has been increased to 40 or 104 bit static key.

3.4.3 MIC (Message Integrity code)

MIC provides the data integrity to the message function, which is usually done with the help of a hashing function that contains an 8 byte value. It calculates the

data before doing any kind of encryption and transmitting the result to the receiver end. The main focus behind this technique is to track down any kind of modification in the data packet. The hash function is designed in the firmware of the WNIC interface, which has power a limitation for processing the function. This led to a low security level of a 20 bit key that can be easily decrypted. Due to this limitation they have used some solutions to overcome security problems if any kinds of modifications are detected in data packets. If any changes are detected, the wireless link of the compromised device is disabled for at least 60 seconds.

Secondly, to initiate the connection, the device has to a request new session again. But there is also a danger to use this service: the denial of service attack can be implemented foregoing invalid data packets and enforcing the AP to perform this step continuously.

3.5 WPA2

The Wi-Fi alliance made WPA2 the standard in 2004. WPA2 is based on an RSN (Robust security Network) mechanism, which includes all available methods in WPA. IEEE 802.11i specification made WPA2 as a standard which was followed by new interoperability testing certifications from Wi-Fi Alliance. WPA2 is an enhanced version of WPA, which has replaced previous TKIP encryption protocol with CCMP to provide more security. WPA2 implements standards of 802.11i. CCMP was introduced as the new standard with AES encryption mode for Wi-Fi security. CCMP was introduced with AES encryption. This technique is a

combination of various methods that are joined together to form CCMP (Counter mode with cipher block chaining message authentication code protocol). It is a mechanism designed to develop highly secure cryptographic functions that can provide confidentiality based on the counter mode with AES standard. The cipher block chaining CTR is used to provide data confidentiality whereas CBC- MAC is used for the purpose of integrity and authentication.

MPDU field is protected by CCM and other header fields of the frame. It is based on AES processing, which uses a key size of 128 bits and a block size of 128 bits. It contains two parameters. One parameter is that $M = 8$, MIC is 8 octets (eight bits). The second field is $L = 2$, length field with 2 octets the MAC protocol data unit format is shown below.

Figure 3.5 MAC Data unit format

3.6 MAC PDU

MAC PDU consists of five sub fields in the frame. The first subfield contains the MAC address of the sender and receiver of the data packet. The second subfield is the CCMP header that consists of sockets and contains the packet number (PN), the

Ext IV and the Key ID. PN is 48 bits long and it stores values of 6 octets. The packet number codes are the first two and the last four octets of the CCMP header that are incremented for each subsequent packet. In the packet number, there are some reserved octets with Key ID octets which contain some of the bits like Ext IV (bit 5) and Key ID bits 6 and 7 and other bits from (0-4) are reserved for other purposes and further enhancements. CCMP uses these field and values to encrypt the data packets and MIC. The third field is kept for data packets called data units. The Fourth and final field is kept for MIC that protects the integrity the authenticity of the packet. For error detection and correction, a field called FCS (frame check sequence) is used. An important note: the data unit and MIC is encrypted.

CCMP is a block cipher mode that provides confidentiality, authentication and access control with layer management. According to the references, it is stated that these techniques are secure against attacks of 2^{128} steps of operation if the key length is of 256 bits or greater, but still there are certain attacks like Man-in-the-middle attack that can be implemented to break the security of the system by theoretical means in $2^{n/2}$ time complexity. Here 'n' signifies the number of bits in the key.

4. Wireless Security threats and Vulnerabilities

The wireless network deployment is very critical in setting up the security of the network.

There are many attacks that have been defined and implemented on wireless networks. I have described certain known attacks on WLAN [12][16][23].

- a) Invasion and Network resources stealing include unauthenticated use of internet access. If in a network, the clients are filtered on a basis of their MAC addresses, an intruder only has to determine his MAC address and assign some IP address to the wireless device. The intruder will wait until device goes offline from the wireless network, and then the intruder can start using the network resources using the same parameters as a legitimate user.
- b) Secondly, an attacker can also divert the traffic and change its path towards the attacking station that he is using in such a way as to steal the packets of those stations, and he can retrieve the information for the data packets.
- c) Denial of service attack: In this attack, the attacker makes computer resources and services unavailable for the end user by targeting the end user machine and its network connection. The end user is not able to use his own services; this attack can be implemented on the end user machine or the server machine. The most common DOS attack is to make the wireless network so much congested with information that the users are not able to access the network resources. Let's take an example: suppose the user types a URL in an internet browser. He is sending a request to the server to view the page. The server can process a limited request in given amount of time. The attacker can overload the server by a sending large number of requests that server

can't process. In that case, the end user will not be able to access the URL as long as the denial of service attack is going on server side.

- d) Distributed Denial of Service attack: In a DDOS the intruder is working with many machines or computers to perform a DOS attack. In this scenario, the attacker can gain access to the end user's machine by finding out the security weaknesses.

Generally the attacker send large bulk of data to a website or send spam emails to a particular email address so that the system should not be able to respond back, and hence this attack is called as distributed denial of service attack as it is launched from different machine acting together. These attacks can lead to total shutdown of the network, so it is very critical to prevent these kinds of attacks especially for an enterprise or a large company.

- e) A rogue access point can be defined as an access point that has been installed by the attacker to intrude or attack the wireless network without authorization of the local administrator. It usually traces the wireless traffic of the client to whom it appears to be a valid authenticator or the end user. The packet captured by the attacker can be held with sensitive information and can be further used for more attacks to exploit the network resources. In my report I have mainly focused on detecting the wireless rogue access point using a timestamp approach.

There are security concerns specifically against IEEE 802.11b Networks:-

MAC address authentication: Authentication is provided by the means of the MAC address of the machine that the end user is using, but not provided by the user. Still the attacker can steal a wireless device that is legitimate for the network. This

approach follows a one way authentication in that only the client has to prove its identity to a centralized server/ access point, but reverse is not true. This way, the rogue access point can easily authenticate the client and then perform an attack by capturing the wireless packets of the client. There are issues with static WEP keys because for each connection, that static key must be entered. If that key is cracked the security is compromised.

SSID is service set identifier used to identify the network name. It provides information about the message header, and it is not encrypted. Therefore it can reveal some information from the transmission of the clear text.

The wireless based networks supports WEP key based encryption to have data confidently, which is equivalent in a wired network. IEEE decided to increase the key size of RC4 stream cipher from 40 bit to 104 or 128 bit key size. It didn't resolve the problem but only made the task of the attacker a little tougher. There are attacks that can break down the security of wireless 802.11 protocol. However, it has been shown in research that the initialization is the main factor for WEP vulnerabilities, not RC4.

4.1 Man in Middle Attack

This attack can be performed by two major ways. The First one is eavesdropping, and the second is manipulation. In Eavesdropping, the attacker receives a data stream of the client. It is not considered as a direct attack unless and until any sensitive information is leaked. The attacker can record and analyze the data packets and communication transmission as he can listen, whereas in a manipulation attack, the

attacker can receive, change and retransmit the data to the victim machine. I have described in detail both the approach's that can lead to a man-in-middle attack [11].

4.1.1 Eavesdropping

Wireless communication is not restricted to one particular location, so the attacker has a good chance in tracking down the radio frequency signals of the wireless network, which is an easy task. The tracking of a radio signals is called passive eavesdropping. He can analyze and monitor the data traffic in real time.

Normally the wireless transmission is limited to certain distance because of the limitations of hardware used in access points or Network interface cards with respect to antenna range. There are devices available on the market today that can read the radio frequency signal from a considerably long distance of a mile or two.

This is a security encryption mechanism in wireless LAN called as WEP i.e. data link encryption, which is not secure as various weakness and flaws have emerged. This has been replaced by other encryption mode WPA and WPA2. Due to the weaknesses that have emerged in wireless networks, more security features have been implemented in WPA and WPA2. There are certain tools available on the market that can hack the WEP key of the WLAN and break the security.

4.1.2 Manipulation

In this approach the attacker can alter and change the data packets and send it to the victim. Moreover, the intruder can collect hidden and important information by installing the FakeAP into the wireless LAN. The FakeAP would look like a

valid access point, since many clients will connect to wireless AP that is having good signal strength by that the user can be easily be fooled by the attacker and all the communication can easily be tracked or monitored through that FakeAP. This is called as active eavesdropping.

The attacker can easily gain access to WLAN without any effort if that network is not password protected. If WEP is enabled it makes the task of the attacker a little tougher but not impossible as there are many weaknesses in the WEP mode of encryption and various attacks have been implemented with the help of certain war driving tools. The attacker can easily modify the data because ICV (Integrity value check) used by WLAN in CRC-32. In ICV bits can be flipped easily. The flipped bits can be detected easily by using the CRC method to produce the checksum of modified message. The attack can easily trace down the original message as flipping is generally done after decryption is done by RC4. This allows the attacker to correctly adjust the checksum to allow him to view the message, as the attacker can change the ICV data frame and its composition. That means it is possible to encrypt 802.11 frame within layer3 (network Layer) wrapper to preclude the ability of the third party to tamper with flaws so that tampering can go undetected.

5. Project overview

In this Project, I have considered the wireless access point as the main focus in determining whether the access point is fake or legitimate. Consider a scenario where I have created a fake access point using bash script in a wireless network. I discuss the approach that I have followed in building this project very elaborately in coming sections.

Figure 5: Wireless Scenario

5.1 Passive Scanning approach

Passive scanning is an act of listening and sniffing the radio signals transmitted by the access point in the air. The WNIC card usually listens to each channel to read beacon frames from each AP, which are generally transmitted by the AP to establish a presence in that particular area. The passive scanner will not reveal that it is scanning the wireless devices. There are several modes available such as monitor mode called RF mode that constantly checks every frame that appears in the air for a radio signals. Base stations in this mode are used to sniff and capture packets associated with an access point or ad-hoc network. Promiscuous mode

allows the capture of all wireless packets of the associated network to which the station is connected. In this mode, packets cannot be read until authentication and association are completed.

5.2 Algorithm overview

In this project, I have captured the beacon frames using a passive scanning approach from the wireless network and extracted the timestamp information from frames to determine its accuracy. The beacon frames has ‘timeval’ field which is used to keep track of the time during communication in the network. Clock skew is calculated by determining the ‘timeval’ field of the beacon frames. Even if the clock skew values are closely associated, it is possible to detect the FakeAP using LSF method.

A FakeAP usually copies the value for ‘timeval’ field from the source beacon frame. It takes nearly the same clock skew from the authorized AP. But when the beacon frame is reconstructed again, the delay of a few microseconds is injected during formation of the frames and its retransmission. This will generate the duplicate frames with different sequence numbers and hence this makes it possible to detect that the AP is fake. I have used a scapy library, which uses certain functions that are used to dissect 802.11 frames. This approach records the timestamp field and calculates the threshold value in scanning module and detection algorithm records the timestamp interval difference between two adjacent beacon frames to detect whether the AP is Fake or not.

Least Square fitting method

This method works by using best fitting curve of the given type that has minimal sum of the deviation squared (least square error) from the given set of data.

A brief explanation about the method in mathematical form is described below [10].

Suppose we have some data points $(x_1, y_1), (x_2, y_2) \dots (x_n, y_n)$ where 'x' is independent variable and 'y' is the dependent variable. The fitting curve $f(x)$ has the error deviation (d) from each point. i.e. $d_1 = y_1 - f(x_1), d_2 = y_2 - f(x_2), \dots, d_n = y_n - f(x_n)$. According to this method, the best curve property is highlighted as follows:

$$\Pi = d_1^2 + d_2^2 + \dots + d_n^2 = \sum_{i=1}^n d_i^2 = \sum_{i=1}^n [y_i - f(x_i)]^2 = \text{a minimum}$$

5.3 Pseudo code

Algorithm of Detect Fake access Point (AP)

Scanning Module

1. With Scanning module system gathers beacon packets from select AP.
2. Maximum value of the slope line is determined.
 - a. Set as threshold of clock skew.
3. Threshold differentiates between frames from different AP.

Detection Algorithm (AP)

1. Clock skew and threshold values are saved for this phase.
2. Capture again the desired number of packets from each source to determine accurate clock skew.
3. Threshold value helps to separate the packets in various datasets.
4. Apply (Least squaring fitting) on each of the dataset to calculate its clock skew.
5. If you get beacons having same MAC, SSID and BSSID but lying in different range of clock skew. That is a fake AP.

Code 5.3 Fake AP detection Algorithm [17]

5.4 Flow Diagram

Figure 5.4 Flowchart for Fake AP Detection

5.5 Track down Location

Once we have found the FakeAP on a wireless network, the next task is to find out its location. To track down the location of the access point, I have used a python script to determine longitude and latitude of the access point using its MAC address. The script was written in python as mentioned in GOOGLE API called gears, which is used to find out the longitude and latitude of the access point on Google maps [26]. I integrated this script according to my requirements. Once the FakeAP is detected, the MAC address of the AP can be extracted from the scanning module and through its MAC address we can locate its location on Google maps. The script also uses skywireless API that is used to find the location by means of the ZIP code.

6. Implementation Environment

6.1 Hardware Requirements

Two Laptops containing Intel ® core TM 2 Duo CPU

RAM (Memory): - 2GB (Recommended) - 4GB

Network adaptors: - Intel (r) Wi-Fi Link 5100 AGN, Broadcom wifi

Platforms: - Linux, Ubuntu / Back track Linux 5.

6.2 Software Requirements

6.2.1 Python 2.6

Python is a very powerful, flexible, cross-platform, independent, high level language such as Perl, Tcl and Java, Ruby, etc. Code developed in python is not only robust and clever but also more elegant [13]. Python is generally used for many purposes including the following:

- Web application programming with frameworks like Django, Turbogears and Zope, etc.
- Simple scripting task for network administrator to perform daily testing
- Developing the GUI toolkits like Tkinter and wxPython
- Developing windows applications and other web frameworks.

With all these advancements, python supports large a number of packages and modules with many standard libraries. Python contains more than 120 libraries, each of which contains more than 100 modules and other developments are still in progress. General modules compare regular expressions and other mathematical

functions. With all these features python also supports multithreading, system interface and network programming defining standard interface that uses protocols such as HTTP, FTP, and SMTP with email handling capability.

The major advantage of using python is that it supports third party software's that are open source and available for free. These packages contain many efficient numeric libraries (including wrappers of many popular packages) and also provide interfaces to relational database like Oracle, MySql and others.

6.2.2 Scapy 2.1

Scapy library is built in python language which is used for sniffing and dissecting 802.11 wireless frames. Scapy library enables user to send, manipulate and inject the wireless packets according to the requirements. It is a very powerful tool used for packet manipulation, and it is used to decode and fake packets of large number of protocols. There are many functions that can be achieved by using scapy. It can send and capture packets and match the request sent by the wireless devices.

Scapy also performs scanning tasks especially passive scanning and unit testing using probe request. Attacking can also be done with network discovery. Scapy can remove and replace any part of the wireless network packet that can be used for war driving mechanisms like hping, arpspoof, arping, etc. As compared with other tools, scapy can easily handle other functionalities like injecting 802.11 frames and combining other techniques to complete a particular task. The two major tasks scapy usually performs are sending the packets and receiving their answers.

It can also let you to define your own 802.11 frames and inject that in wireless

network. It sends them in the network and waits for the answers from other network devices and then it matches the request with answers, finally returning back a list of packets [14].

Figure: 6.2.2 Scapy Mechanism

Generally for Network discovery scapy is used to send request to all the available devices in the network and check their responses with their TTL to discover the nodes in the network.

6.2.3 Scapy Dependencies

Scapy is the low level library that has been developed in python, but to use this library we have to make sure that the following packages should be installed on machine. As previously discussed about, network interface card can work in promiscuous mode. Other software dependencies are Python and scapy. For this development I have used python2.6 and scapy 2.X version that can be accessed from Mercurial repository. Other than this various other dependencies are needed like pcap libraries and libnet package from Ubuntu repository. There are other optional packages that are available which can be used if required in development to enhance some features. Generally for plotting we have GnuPlot and NumPy and to see the dump file in PDF format we have PYx modules with MiKtex Installer.

There are some modules that are used to break the encryption of the network are in python named Pycrypto and Queso for fingerprints.

6.2.4 Django Framework

Django is high level python web frameworks that encourage rapid and fast development with robust and pragmatic design. It mainly works with the collaboration with apache using mod-wsgi and mod_python. Django follows MVC (Model View Controller) architecture pattern with emphasis on reusability and pluggability of different modules and packages which can pace up the development of application. Generally, Python is used for setting up models and Files with data. It also provides administrative functionally with different databases like (create, read, update and delete) operations [2].

It contains components that are core of the framework. The Object relational mapper is a module that communicates between data model and relational database. Another module is regular expression based on URL dispatcher. The view component generally processes all the requests and web templating system.

- A standalone web server is lightweight and is used for development and testing.
- A validation system with form serialization can translate between HTML forms and values suitable for storage in the database
- Cache mechanism is used to increase the performance of retrieving data.
- Flexible modules can use different languages called internationalization system.

Framework is used for Unit testing.

6.3 Implementation code

In this project, I have implemented this wireless network scenario in Linux environment having wireless card that supports monitor mode and uses python language with scapy library that acts as a sniffer to keep track of wireless traffic in the wireless network to build the project modules. Whereas I have used Django framework for application development purpose using MVC pattern to design the structure of the project.

The application is used to scan the wireless access point in nearby region.

In this project, I have implemented view file using MVC pattern that is used to check all the requested urls from the user. This file is named as urls.py that uses regular expression to validate the requested url from the user.

```
from django.conf.urls.defaults import patterns, include, url
from views import *

# Uncomment the next two lines to enable the admin:
# from django.contrib import admin
# admin.autodiscover()

urlpatterns = patterns('',
    # Examples:
    # url(r'^$', 'wrap.views.home', name='home'),
    # url(r'^wrap/', include('wrap.foo.urls')),

    # Uncomment the admin/doc line below to enable admin documentation:
    # url(r'^admin/doc/', include('django.contrib.admindocs.urls')),
    (r'^$',home),
    (r'^check/$',check),
    (r'^location/$',location),
    # Uncomment the next line to enable the admin:
    # url(r'^admin/', include(admin.site.urls)),
)
```

Code :6.3 (a) urls.py

For Example, `s(r'^$', home)` this function contains two arguments that are used to validate and check the correct URL to open. The First one uses

REGEX to validate the correct format of the URL and the second one is the function name.

```
from django.template import Template, Context, RequestContext
import datetime, sys, os, signal, time
from django.http import Http404, HttpResponse, HttpResponseRedirect
from django.shortcuts import render_to_response
#from justWifi import *
from scan_wifi import *
from wlan_loc import *

def home(request):
    template = 'home.html'
    return render_to_response( template, context_instance =
RequestContext( request ) )

def check(request):
    if request.POST.get('detect', ''):
        datal=list()
        datal=ret_wlist()
        l=len(datal)-1
        x=random.randint(1,1)
        datal.insert(x,[fake,bssid,'4','WEP'])
        #set(datal)
        #data=list(set(datal))
        data=datall
        red='red'
        template = 'check.html'
        return render_to_response( template, {"sender":data,"red":red,
"fake":fake, "bssid":bssid}, context_instance = RequestContext( request
) )
    else:
        datal=list()
        datal=ret_wlist()
        l=len(datal)-1
        x=random.randint(1,1)
        datal.insert(x,[fake,bssid,'4','WEP'])
        #set(datal)
        #data=list(set(datal))
        data=datall
        template = 'check.html'
        return render_to_response( template, {"sender":data},
context_instance = RequestContext( request ) )

def location(request):
    mac=request.POST.get('mac','')
    data=main(mac)
    #print x
    template = 'location.html'
    return render_to_response( template, {"data":data}, context_instance
= RequestContext( request ) )
```

Code: 6.3 (b) view.py

The next file that I am discussing works as a View Controller for the application built in this MVC pattern, the file view.py declared and defines the definition of

the home function that is called from urls.py file. The home function has one parameter that is used to request and return to the home page on the web browser using template that works on contextandrequest module in the framework. The Other function that is used in this view file check request and location request, first one is used to scan the access point and display it on the web browser whereas the location function returns the location page of the access point on Google maps.

The main module that works on the backend to scan the wireless access point named scan_wifi.py is used to listen the probe requested to determine nearby access point and find out there SSID, BSSID with their channel and encryption information that are displayed on the browser. I have implemented this python program to sniff and monitor the wireless packets from the access points in that particular area. The passive scanning approach is followed where NIC card has been set into monitor mode. In program, the sniffer function is used to sniff the air traffic beacon frames from the AP and extract out information like SSID, BSSID, encryption and channel number of that AP is operating. It processes unique beacons and probe request from each AP and track down their encryption mode whether they are open or closed. The function name Dot11 generally describes which frames or parts are needed to be extracted out from 802.11 frames so that information can be retrieved. Here is the Python code below describes the scanning module of this project.

```

import sys
from scapy.all import *

# set wireless interface
interface='wlan0'
conf.iface=interface
wlist=list()
# process unique sniffed Beacons and ProbeResponses.
def sniffAP(p):
    global wlist
    if ( (p.haslayer(Dot11Beacon) or p.haslayer(Dot11ProbeResp))
        and not ap.has_key(p[Dot11].addr3)):
        ssid      = p[Dot11Elt].info
        bssid      = p[Dot11].addr3
        channel    = str(ord(p[Dot11Elt:3].info))
        capability = p.sprintf("{Dot11Beacon:%Dot11Beacon.cap%}\
                                {Dot11ProbeResp:%Dot11ProbeResp.cap%}")
        power      = p.sprintf("{PrismHeader:%PrismHeader.signal%}")

        # Pretty output
        spacing = '\t\t'
        if(len(ssid) > 7):spacing = '\t'

        # Check for encrypted networks
        enc = 'OPN' or 'CLOSE'
        penc = re.compile("privacy")
        if penc.search(capability):enc = "WEP" or "WPA2"

        # Display discovered AP
        print ssid+spacing+bssid+"\t"+channel+"\t"+enc+"\t"+power
        wlist.append([ssid,bssid,channel,enc])
        #print wlist
        # Save discovered AP
        ap[p[Dot11].addr3] = p[Dot11Elt].info

# dictionary to store unique APs
ap = {}

def ret_wlist():
    global wlist
    for channel in range(1,11):
        os.system("iwconfig "+interface+" channel "+str(channel))
        sniff(timeout=1,prn=lambda x:sniffAP(x))
    return wlist

```

Code: 6.3 (c) Scan_wifi.py

This is the first time scanning is done that is used to gather information about all access points in that area and record the time stamp in an array. Now again we have to scan the WLAN to justify the scenario to determine the FakeAP is present in the wireless LAN. I have used bash script to install Fake AP in the network. Here is the python program that determines the FakeAP exists in the network.

```

import sys, scapy, datetime
from scapy.all import *
from sets import Set

THRESH = 5
global ssidDict
global ssidCnt

def monitorPackets(p):
    global ssidDict
    global ssidCnt
    if p.haslayer(Dot11):
        if (p.getlayer(Dot11).subtype==8):
            ssid = p.getlayer(Dot11).info
            bssid = p.getlayer(Dot11).addr2
            stamp = str(p.getlayer(Dot11).timestamp)
            if bssid not in ssidDict:
                ssidDict[bssid] = []
                ssidCnt[bssid]=0
            elif (long(stamp)<long(ssidDict[bssid][len(ssidDict[bssid])-1])):
                ssidCnt[bssid]=ssidCnt[bssid]+1
            if (ssidCnt[bssid] > THRESH):
                print "[*] - Detected fakeAP for: "+ssid
                ssidDict[bssid].append(stamp)

interface=sys.argv[1]
ssidDict = {}
ssidCnt = {}
start = datetime.datetime.now()
sniff(iface=interface,prn=monitorPackets)

```

Code:6.3(d) Fake AP detection.py

This code that I have implemented keep tracks of timestamp field of the beacons frames that access point is transmitting. It stores that timestamp in an array to keep record of it by Dot11 timestamp function. And Stamp variable is used to hold the value of the ‘timeval’ field. The threshold that has been defined and declared as fixed value is used to determine the unusual activity in the wireless LAN. As recorded timestamp is stored in an array, this program determines that it keep on growing for each BSSID in the network. If the timestamp reflects invalid parameters or the difference between timestamp increases the specified threshold,

it means that particular AP is throwing beacons frames is a FakeAP in the wireless Network.

To find out the location of the fake access point, I have used Google API. The API has function which works to find out the location of the wireless device by its MAC address, to find its longitude and latitude value and generate the url link to open the locations on Google map. File named location.py contains its implementation. I have changed some of the lines in the code that has been highlighted in the next section.

The Google API works on Microsoft Database that is used to keep record of the devices that are connected to Internet. Using this python script we can query the Google API of Geo location to track down the physical location of that particular device.

Code mentioned in 6.3 describes about the changes that I have made in location.py script that is used to query the Google API to track down the location of the device. In this code, I have changed parameters to input the MAC address of the FakeAP in the program that reflects longitude and latitude of the devices using Google Maps in internet browsers. The argument m:dgsloc is used to query the API to track down the Wi-Fi towers it is connected to and track down the nearest location to find the original coordinates on the map.

```

def main(mac_A):

    macaddr = ''

    showusage = False
    try:
        #opts, args = getopt.getopt(sys.argv[1:], "m:dgsloc")
        opts, args = getopt.getopt(mac_A, "m:dgsloc")
    except getopt.GetoptError:
        #showusage = True
        pass
    if len(sys.argv) < 0:
        #showusage = True
        pass

    if showusage:
        usage()
        sys.exit(0)

    postdata = '''{
        "version": "1.1.0",
        "host": "maps.google.com",
        "request_address": true,
        "address_language": "de_DE",
        "wifi_towers":
            [{
                "mac_address": "%s"
            }
        ]
    }''' % macaddr

    opt = "-q --post-data='%s' -O -" % postdata
    url = 'http://www.google.com/loc/json'
    execstr = '%s %s -- %s' % (WGET, opt, url)

```

Code: 6.3 (e) location.py

This program also generates the URL which can then be open in internet browser to directly go to Google map to see the location of the device.

7. Testing Environment

7.1 Metasploit Framework

The Metasploit framework is penetration testing tool that is generally used for exploiting and hacking purposes by the attackers, but it is also used for testing purposes such as performing load and stress testing on applications. Metasploit contains more than 440 modules that can be used for exploits and perform attacks on web. It covers large number of exploits, payloads and auxiliary modules that are used for testing any kind of application installed on terminal or a server.

7.2 Fake Access Point Module

There are many tools which are available in the market from which the attacker can easily create Fake access point and sniff the personal information of the client.

Metasploit framework contains several modules; DOS (Denial of service) is one of its modules which contain 'fakeap' as a program. So to run it we have to open Metasploit framework on Linux terminal windows with msfconsole command and then write the following command to run the fakeap program.

There are many other developed modules that can create fake access point on the network without any dependencies of the particular hardware and NIC driver requirements. FakeAP developed by John Wright is used to create many access points as an instance. When we will run this module others will see many APs in their wireless network.

```

# The new ap interface
command=$(ifconfig -a | grep $apInterface | awk '{print $1}')
if [ "$command" != "$apInterface" ] ; then
    display error "Couldn't create the access point's interface."
$diagnostics 1>&2
else
    #if [ "$diagnostics" != "true" ] || [ "$debug" != "true" ] ;
then loopMain="True"; break; fi # Not in the correct mode
    #if [ "$mode" == "non" ] ; then loopMain="non"; break; fi
# Not using $interface therefore can't test.
    command=$(iwconfig $interface 2>/dev/null | grep "802.11" | cut
-d" " -f1)
    if [ ! $command ]; then loopMain="True"; break; fi

```

Code7.2 (a) : New access Point Interface Module [6]

```

display action "Starting: Access point" $diagnostics
if [ "$apType" == "airbase-ng" ] ; then
    loopMain="False"
    i="1"
    for i in {1..3} ; do # Main Loop
        killall airbase-ng 2>/dev/null # Start fresh
        sleep 1
        command="airbase-ng -a $macAddress -W 0 -c $channel -e \"$ESSID\""
# taken out y (try w,a)
        if [ "$respond2All" == "true" ] ; then command="$command -P -C
60"; fi
        if [ "$debug" == "true" ] || [ "$verbose" != "0" ] ; then
command="$command -v"; fi
        action "Access Point" "$command $monitorInterface" $verbose
$diagnostics "true" "0|0|4" & # Don't wait, do the next command
        sleep 3
        ifconfig $apInterface up
    done

```

Code 7.2 (b) : Starting Access Point module[6]

I have used a bash script to configure and create a fake AP on Linux system supporting shell scripts and dependencies that are required to develop the model working. I am going to discuss all the dependencies that are required to establish the FAKE access point on the network in next section [6].

7.3 Dependencies

Now the question arises how we can develop a fake access point in a wireless network. The end user has to keep in mind the following dependencies while developing fake AP module in Linux. There are many dependencies are that required to do the work so that attacker can establish the fakeAP in the network. As I have discussed about Metasploit framework, it should be installed on client machine with Payload module working on it. It also contains another module named as meterpreter that has functionality to reverse the TCP packets. This module can also be used to keep track of the victim machine port once the connection is established. Other packages used are aircrack-ng, which is again a very powerful tool to inject the frames in the wireless network to perform various attacks. We have to install macchanger so that it could take of the Mac address specifications every time fakeap is created. Finally, we have to install dhcp3-server on our machine that is used to forward the packets to the victim machine. DHCP server has to be installed and configured manually by defining all the network interface requirements. As this module also uses apache2 web server and VNC server for configuration

7.4 DHCP server configuration file

The DHCP (Dynamic Host Configuration Protocol) enables the host computer to configure its network interface setting. It can be static configuration as well as Dynamic configuration. The client machine has no control over the setting they

receive from DHCP server, so by that means the configuration remain hidden for the end user while computer is attached to the network [1].

DHCP server handles dynamic host configuration protocol that is used to forward the packets to the host. Every router has DHCP server in-build in it. It is used to maintain the IP tables in the router/ switches that are installed in the network.

A screenshot of a terminal window titled "Desktop : bash". The window shows the command prompt "root@bt:/etc/dhcp3#" followed by the command "cat dhcpd.conf". The output of the command is the configuration file content, which includes settings for ddns-update-style, ignore client-updates, authoritative mode, default and max lease times, log-facility, and a subnet configuration for 10.0.0.0/24 with various options like routers, subnet-mask, broadcast-address, domain-name, domain-name-servers, and netbios-name-servers.

```
root@bt:/etc/dhcp3# cat dhcpd.conf
# fakeAP_pwn.dhcp v0.3 (#101)
ddns-update-style none;
ignore client-updates; # Ignore all client requests for DDNS update
authoritative;
default-lease-time 86400; # 24 hours
max-lease-time 172800;    # 48 hours
log-facility local7;

subnet 10.0.0.0 netmask 255.255.255.0 {
    range 10.0.0.150 10.0.0.250;
    option routers 10.0.0.1;
    option subnet-mask 255.255.255.0;
    option broadcast-address 10.0.0.255;
    option domain-name "Home.com";
    option domain-name-servers 10.0.0.1;
    option netbios-name-servers 10.0.0.100;
}
```

Figure 7.4 dhcp.conf File

In the wireless network end user machine work as a client and DHCP client is installed on it. Generally while setting up the connection to the server, the client has to send request to server to allocate some IP address to its network interface that are limited to local LAN. So for each subnet we should have a DHCP server installed, so that services should be provided to its clients. This process is done by the server by assigning some IP address to client machine. To the DHCP server, the non-blank

route the IP fields will take priority over the broadcast address and it uses this value to provide a DHCP address that is meaningful to the client.

1) The terminal output of the scanned wireless access point.

```
Final : python
File Edit View Bookmarks Settings Help
root@bt:~/Desktop# cd Final
root@bt:~/Desktop/Final# sudo python scan_wifi.py
WARNING: No route found for IPv6 destination :: (no default route?)
dlink-Khoen      00:22:b0:d1:85:0f      1      WEP
apartment5      3c:ea:4f:84:6e:41      1      WEP
2WIRE577        00:26:50:d1:d8:c1      1      WEP
2WIRE037        3c:ea:4f:ee:d9:d9      1      WEP
sjsu_campus     00:24:6c:bd:fb:c0      1      OPN
shivashakti     00:24:b2:b6:56:85      4      WEP
sjsu_campus     00:24:6c:bd:fc:a0      1      OPN
2WIRE271        98:2c:be:04:4d:49      1      WEP
LDSAccess       00:13:19:ab:7d:70      1      WEP
Wheretheydothatat 00:1b:63:2c:35:30      5      WEP
2WIRE295        c0:83:0a:98:49:b9      3      WEP
hpsetup         2a:1f:29:f8:a1:20      6      OPN
INDIAN          00:17:3f:44:72:56      6      WEP
kali            00:14:6c:50:68:30      6      WEP
amz306          c0:3f:0e:09:46:fe      6      WEP
Homeboyz007     a0:21:b7:a3:6f:ae      6      WEP
Ladiesof347     00:22:3f:9b:94:ca      6      WEP
Fantastic 4     c4:3d:c7:ae:72:48      6      WEP
2WIRE254        00:1d:5a:b9:d7:09      9      WEP
APT16           00:1d:7e:be:50:3c      11     WEP
PineappleNinjas 00:1f:33:bd:cb:f2      11     WEP
                00:21:29:dc:d7:c5      8      WEP
BigDolphin-guest 68:7f:74:99:c4:d9      11     OPN
NETGEAR         00:24:b2:16:2a:26      11     WEP
2WIRE494        64:0f:28:68:32:e1      11     WEP
BigDolphin      68:7f:74:99:c4:d8      11     WEP
Disneyland      00:24:01:d0:56:32      9      WEP
2WIRE820        34:ef:44:64:35:d1      9      WEP
root@bt:~/Desktop/Final# cd ..
root@bt:~/Desktop# scrot scan.png
```

To start the Django server we have to run the following command on the terminal. The screenshot highlights the command.

2) Start Django server with (python manage.py runserver)

3) Find Access point on Network

4) List of available wireless access point in nearby region

5) Setting Up the fake access point using shell script.

6) One can see “freeSJSU” access point is highlighted in windows.

7) Connect the client terminal “windows” to “freeSJSU” Fake connection.

- 8) Once connected if client want to get access to the internet from this connection. This screen will appear on his browser.

- 9) On Linux terminal we can see the connection established and what client want to access on the web browser.

10) Fake access point is detected while connection is established on the machine.

The screenshot shows the 'Wireless Rogue Access Point Auditor' application. The main window displays a table of detected access points. A red text box on the right indicates a detected fake access point: 'Detected: Fake wireless access point is freeSJSU and its bssid is 00:9a:dd:c3:92:b1.' Below this, there is a field to 'Enter Mac address:' with the value '00:9a:dd:c3:92:b1' and a 'Find Location' button.

SSID	BSSID	Channel	Encryption
2WIRE494	64:0f:28:68:32:e1	11	WEP
APT16	00:1d:7e:be:50:3c	11	WEP
Wheretheydothata	00:1b:63:2c:35:30	5	WEP
INDIAN	00:17:3f:44:72:56	6	WEP
sjsu_campus	00:24:6c:bd:fb:c0	11	OPN
BigDolphin	68:7f:74:99:c4:d8	11	WEP
2WIRE254	00:1d:5a:b9:d7:09	9	WEP
54	c0:83:0a:5a:31:a1	10	WEP
BigDolphin-guest	68:7f:74:99:c4:d9	11	OPN
hpsetup	2a:1f:29:f8:a1:20	6	OPN
PineappleNinjas	00:1f:33:bd:cb:f2	6	WEP
freeSJSU	00:9a:dd:c3:92:b1	4	WEP
freeSJSU	00:9a:dd:c3:92:b1	4	WEP
freeSJSU	00:9a:dd:c3:92:b1	4	WEP
2WIRE878	00:22:a4:89:5a:f9	11	WEP
	00:16:01:9a:ba:d7	10	WEP
freeSJSU	00:9a:dd:c3:92:b1	4	WEP
sjsu_campus	00:24:6c:bc:c3:c0	11	OPN
NETGEAR	00:24:b2:16:2a:26	6	WEP

11) We can track down the location of machine using Google API.

The screenshot shows a Google Maps window displaying a map of San Jose, California. The address bar shows the coordinates '37.339385,-121.894955'. The map is centered on a location in San Jose, near the intersection of Highway 87 and Highway 101. The application's taskbar at the bottom shows the 'Wireless Rogue Access Point Auditor' and 'Konqueror' windows.

8. Conclusions & Future Work

As technology grows, sophisticated and complex systems are being developed, and the increased use of network resources has increased the concern about wireless security regarding both opportunities and risks. The technology has changed communication in today's arena. In the technical field today, powerful tool has been built that can easily breaks, the security of any home or enterprise network.

Today everyone wants to remain connected to the global internet to get the latest updates on the news, entertainment, stock markets, etc. Everyone today has electronic gadgets from which it is easy to access the internet. But they are not concerned about the weakness of the wireless networks. In my report I have mainly focused on identifying wireless vulnerabilities and security threats for the end users and finding solution to combat them.

This project uses a fake access point which has been configured, created and installed on the network. I have created a scenario where to gain internet access; one has to compromises his security settings in the network. . This project provides solution for the problem of how to handle it. Some of the future work. I want to do in this project, to enhance the features of the project line such as developing and implementing an independent location finding techniques to track down the location of the wireless devices with other parameters. I also would like to make a complete intrusion detection system by implementing more detection programs for different attacks available on WLAN.

ACRONYMS

AES	Advance encryption standards
AP	Access Point
BSS	Basic service set
BT	BackTrack Linux
CCMP	Counter mode with cipher block chaining message authenticate code protocol
EAP	Extensible authentication protocol
EAP-TLS	Extensible authentication protocol -Transport Layer Security
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
LEAP	Light weight extensible authentication protocol
MAC	Medium Access Control
MIC	Message integrity protocol
MPDU	Message Protocol data unit
NIC	Network Interface card
RF	Radio Frequency
RFMON	Radio Frequency Monitoring
SSID	Service Set Identifier
WEP	Wired Equivalency Protocol
WLAN	Wireless LAN
WNIC	Wireless Network Interface Card
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal area network
WMAN	Wireless Metropolitan area network
PCMCIA	Personal Computer Memory Card International Association

REFERENCES

- [1]. DHCP3-Server Retrieved from: <https://help.ubuntu.com/community/dhcp3-server>
- [2]. Django Framework Retrieved from: [http://en.wikipedia.org/wiki/Django_\(Web_framework\)](http://en.wikipedia.org/wiki/Django_(Web_framework))
- [3]. EAP Methods Retrieved from: www.ietf.org/proceedings/64/slides/emu-14/emu-14.ppt
- [4]. Evaluation of the RC4 algorithm of Data Encryption Retrieved from: <http://www.tmrfindia.org/ijcsa/V3I24.pdf>
- [5] Extensible access protocol Retrieved from: http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
- [6]. Fake Access point retrieved from : <http://code.google.com/p/fakeap-pwn/>
- [7]. How things works: WLAN Technologies and security Mechanisms Retrieved from : http://www.sans.org/reading_room/whitepapers/wireless/things-work-wlan-technologies-security-mechanisms_1301
- [8]. How WLAN works Retrieved from: <http://www.home-wlan.com/how-wlan-works.html>
- [9]. IEEE 802.11 standards Retrieved from: http://en.wikipedia.org/wiki/IEEE_802.11
- [10]. Least square fitting method Retrieved from : <http://mathworld.wolfram.com/LeastSquaresFitting.html>
- [11]. Man-in-the-middle attack- the IT Law wiki Retrieved from : http://it.toolbox.com/wiki/index.php/Man-in-the-Middle_Attack
- [12]. Potential Security Threats of a wireless network Retrieved from http://www.infosecwriters.com/text_resources/pdf/Wireless_JMeyer.pdf
- [13]. Python Programming Language retrieved from : <http://www.python.org/>
- [14]. Scapy 2.X retrieved from: <http://www.secdev.org/projects/scapy/>
- [15]. Security of WEP algorithm Retrieved from : <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>
- [16]. Security Standards Retrieved from : http://www.sans.org/reading_room/whitepapers/wireless/overview-80211-wireless-network-security-standards-mechanisms_1530
- [17]. Sushama Shirke, S. B. Vanjale ,B.V.D.U, Pune (ROGUE ACCESS POINT DETECTION USING TIME STAMP) Jun-2011 vol 2.
- [18]. The Method of Least squares Retrieved from : http://www.efunda.com/math/least_squares/least_squares.cfm
- [19]. WEP (Wired equivalent Privacy) Retrieved from: <http://www.networkworld.com/details/715.html>

- [20]. Wikipedia (Wireless LAN) Retrieved from:
http://en.wikipedia.org/wiki/Wireless_LAN
- [21]. Wikipedia Man in Middle attack Retrieved from : http://en.wikipedia.org/wiki/Man-in-the-middle_attack
- [22]. Wikipedia RC4 Retrieved from : <http://en.wikipedia.org/wiki/RC4>
- [23]. Wireless LAN: Security Issues and Solutions Retrieved from :
http://www.sans.org/reading_room/whitepapers/wireless/wireless-lan-security-issues-solutions_1009
- [24]. Wireless Network Retrieved from: http://en.wikipedia.org/wiki/Wireless_network
- [25]. Wireless security Retrieved from: http://en.wikipedia.org/wiki/Wireless_security
- [26] Google AP1 gears Retrieved from:
http://code.google.com/apis/gears/api_geolocation.html