“Rogue Access Point Detection Using Multi Parameter Dynamic Feature Analysis for Wireless LAN”

A THESIS SUBMITTED TO

BHARATI VIDYAPEETH DEEMED UNIVERSITY, PUNE

FOR AWARD OF DEGREE OF

DOCTOR OF PHILOSOPHY IN
COMPUTER ENGINEERING

UNDER THE FACULTY OF ENGINEERING AND TECHNOLOGY

SUBMITTED BY

MR. SANDEEP B. VANJALE

UNDER THE GUIDANCE OF

PROF. DR. P. B. MANE

RESEARCH CENTRE

BHARATI VIDYAPEETH DEEMED UNIVERSITY,
COLLEGE OF ENGINEERING, PUNE-43

AUGUST 2016

CERTIFICATE

This is to certify that the work incorporated in the thesis entitled **“Rogue Access Point Detection Using Multi Parameter Dynamic Feature Analysis for Wireless LAN”** for the degree of **‘Doctor of Philosophy’** in the subject of **Computer Engineering** under the **Faculty of Engineering and Technology** has been carried out by **Mr. Sandeep B. Vanjale** in the **Department of Computer Engineering** at **Bharati Vidyapeeth Deemed University, College of Engineering, Pun**e during the period from **June 2009 to August 2016** under the guidance of **Prof. Dr. P. B. Mane.**

Place: Pune

(Prof. Dr. A. R. Bhalerao)

Date:

Principal and Dean

CERTIFICATION OF GUIDE

This is to certify that the work incorporated in the thesis entitled **“Rogue Access Point Detection Using Multi Parameter Dynamic Feature Analysis for Wireless LAN”** Submitted by **Mr. Sandeep B. Vanjale** for the degree of **‘Doctor of Philosophy’** in the subject of **Computer Engineering** under the **Faculty of Engineering and Technology** has been carried out in the **Department of Computer Engineering**, **Bharati Vidyapeeth Deemed University College of Engineering, Pune** during the period from **June 2009** to **August 2016** under my direct supervision/ guidance.

Place: Pune	**(Prof. Dr. P. B. Mane)**
Date:	Guide and Professor
	Department of E and TC,
	AISSMS IOIT, Pune.

DECLARATION BY THE CANDIDATE

I hereby declare that the thesis entitled **“Rogue Access Point Detection Using Multi Parameter Dynamic Feature Analysis for Wireless LAN”** submitted by me to the Bharati Vidyapeeth University, Pune for the degree of **Doctor of Philosophy (Ph.D.)** in **Computer Engineering** under the **Faculty of Engineering and Technology** is original piece of work carried out by me under the supervision of **Prof. Dr. P. B. Mane.** I further declare that it has not been submitted to this or any other university or institution for the award of any degree or diploma.

I also confirm that all the material which I have borrowed from other sources and incorporated in this thesis is duly acknowledged. If any material is not duly acknowledged and found incorporated in this thesis, it is entirely my responsibility. I am fully aware of the implications of any such act, which might have been committed by me advertently or inadvertently.

Place: Pune

Date:

(Mr. Sandeep B. Vanjale)
Research Scholar
Bharati Vidyapeeth
Deemed University, Pune-30.

ACKNOWLEDGEMENT

I would like to express my deepest appreciation to all those who provided me a great support throughout the research journey. First and foremost, I express my deep sense of gratitude to my research guide **Prof. Dr. P. B. Mane**, Principal, AISSMS IOIT, Pune, for his inspiring guidance, invaluable thought provoking suggestions, constant encouragement and unceasing enthusiasm at every stage of this research work. I am deeply indebted to **Hon. Dr. Patangraoji Kadam**, founder, Bharati Vidyapeeth, **Hon. Dr. Shivajirao Kadam**, Vice Chancellor, Bharati Vidyapeeth University and **Dr. Vishwajeet Kadam**, Secretary, Bharati Vidyapeeth from whom I received continual encouragement and advice. I express my sincere thanks to them. I express my indebtedness to **Prof. Dr. Anand R. Bhalerao**, Dean, Bharati Vidyapeeth University, Principal, College of Engineering, Pune, for providing necessary support during this research work.

I am grateful to Dr. Agav, Dr. V. K. Pachghare of COEP Pune and Dr. S. M. Chavare, Dr. S. T. Patil, Mr. Atul Dhaygude for providing their valuable guidance as well as suggestions.

I am thankful to all staff members of Computer Engineering Department for their support.

Above all I am extremely grateful to my wife, Mrs. Mousami Vanjale who has always been with me during the entire period of this research work. I give special love to my son Paras for his excellent co-operation. Their loving and caring attitude has been the driving force in this endeavor and no words of thanks are enough. I am grateful to my late parents for their blessings and special thanks to my brother, sister, father in-law and mother in-law for their unconditional love and blessings.

I am very much thankful to all my colleagues, relatives, friends and well-wishers for their timely co-operation and support.

Mr. Sandeep B. Vanjale

DEDICATED

TO MY LATE PARENTS

SHRI. BHARATKUMAR B.VANJALE

MRS. LALITA B.VANJALE

AND

MY WIFE MOUSAMI AND SON PARAS

INDEX

CONTENTS

ABSTRACT

Wireless LANs are an integral part of today's globalized economy. WLANs are growing and so are their threats. The main security threat in a wireless network is a malicious or Rogue Access Point (RAP). It is also observed that out of total available Access Points (AP) on the network, almost 20 % APs are unauthorized. Enormous security risks are involved when users connect to RAP which steals sensitive information from the network.

The traditional approach to it is based on the concept of matching of various parameters from beacon frames. It verifies the attributes of APs like MAC address and SSID. In server based approach, RAP detection software is installed on a central server, which analyzes the whole network and performs an operation for detection of RAP. Client based approach has a pre-installed software on the device, which continuously monitors the network and before connecting to an AP, it verifies all the details of that AP to judge if that AP is authorized or not. Present research methods use diverse parameters such as clock skew, wireless traffic monitoring, encryption, authorization, timing based approach, RSS analysis, bottleneck bandwidth analysis, and sequential hypothesis test.

The limitations of the existing methods include; weak clock skew solution assumption; variable inter packet arrival time; mobile agent code cannot be installed on all nodes; MAC and SSID address can be spoofed; variable received signal strength; the system will not work properly if central server is down. These limitations have motivated us to develop a multi parameter based technique to improve the detection of RAP in WLAN.

A robust RAP detection technique is developed by integrating multiple parameters into one solution. Use of sequence count and timestamp as an additional parameter for RAP detection is the main contribution of the implemented solution. The developed system operates in two modes learning and detection mode. The Learning Mode is used to create an authorized AP list (White List). The Detection Mode is used for detection of RAP within a wireless network.

From the results it is observed that the developed multi-parameter based method shows improvement in terms of accuracy of detecting RAP; time required for detecting RAP and primary memory utilization. The accuracy is improved by 2.77% and the detection time is improved by 37.33%, in comparison to the method in reference paper. It is also observed that the primary memory required to run the program is only 16%.

Abbreviations and Notations

Abbreviation/ Notation	Description
AP	Access Point
ACL	Access Control List
AES	Advanced Encryption Standard
BS	Base Station
BSS	Basic Service Set
CD	Collision Detection
CRC	Cyclic Redundancy Checksum
CSMA	Carrier Sense Multiple Access
DAIR	Dense Array of Inexpensive Radios
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
ESS	Extended Service Set
FAP	Fake Access Point
HCI	Host Controller Interface
HDT	Hop Differentiating Technique
HTTP	Hyper Text Transfer Protocol
IBSS	Independent Basic Service Set
ICMP	Internet Control Messaging Protocol
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
LAN	Local Area Network
LPM	Linear Programming Method
LSF	Least Square Fitting
LDAP	Lightweight Directory Access Protocol

Abbreviation/ Notation	Description
MA	Mobile Agent
MAC	Media Access Control
MITM	Man-In-The-Middle
NADS	Network Attack Detection System
NAT	Network Address Translation
NIC	Network Interface Card
PPM	Parts Per Million
PSK	Pre-Shared Key
QoS	Quality of Service
RAP	Rogue Access Point
RAPDL	RAP Detection and Localization
RSNA	Robust Security Network Association
RSS	Received Signal Strength
RTT	Round Trip Time
SDP	Service Discovery Protocol
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
TMM	Training Mean Matching
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
Wi- Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA 2	Wi-Fi Protected Access Version 2

LIST OF FIGURES

LIST OF TABLES

CHAPTER - 1

INTRODUCTION

CHAPTER – 2

LITERATURE REVIEW

CHAPTER –3

DESIGN AND DEVELOPMENT OF RAP DETECTION TECHNIQUES

CHAPTER -4

DESIGN OF THE MULTIPARAMETER RAP DETECTION METHOD

CHAPTER -5

EXPERIMENTAL RESULTS AND ANALYSIS

CHAPTER-6

CONCLUSION

CHAPTER-1

INTRODUCTION

1.1 Introduction

The increase in the number of smartphone users in the world has been impressive. There is a rapid growth of users who use Wi-Fi through mobile devices. Especially devices like tablets are connected only through Wi-Fi. All these devices connected to the wireless network through a device are called as Wireless Access Points (WAP). The access point (AP) is the strength of a wireless network, which helps in providing various usages on wireless surrounding. AP is much popular due to its features such as scalability, cost effectiveness, easy installation, configuration and most important of all, its mobility. Internet connectivity is of utmost important today in every organization. Wireless LAN plays crucial role in providing internet connectivity in networks. The WLAN mostly works at data link layer by providing access to media channels to every competing station. This gives flexibility to network administrators while designing complex networks. Many organizations have confidential data which they regularly use in networks. Events like data leakage over wireless LAN could jeopardize data security of any organization. Presence of RAPs posing as an authorized one is major reason behind data leakage over wireless LAN. Hence detection of RAP is very important in initial stages of wireless LAN implementation.

Utilization of Wi-Fi in public has reached a point where it is tough to avoid intrusion. Kaspersky [41] conducted a global poll about Wi-Fi security, and the result shows that more than 32% of users use public Wi-Fi without paying heed to security concern. A malicious attacker creates a Rogue Access Point (RAP) in a wireless environment. The main target of these attackers is to disturb the network and try to steal sensitive information. A report from AirTight [40] presents that insufficient information regarding secured wireless network, can cause various threats on security. Measure security threats in a wireless network is RAP. As shown in figure 1.1 almost 20% of the total existing APs on the network are rogue.

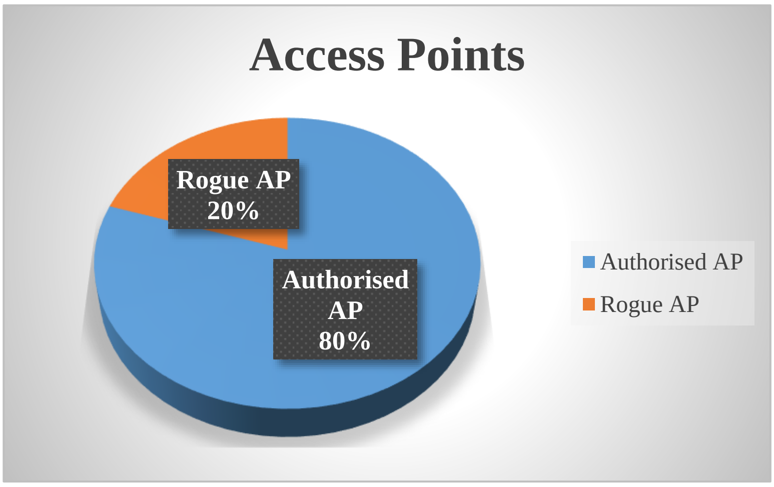


Figure 1.1: Authorized vs. Rogue AP in WLAN

Most of the times internal organizational networks are connected to external networks over VPN. Presence of RAP could create severe threat to organizational data security as data leakage can take place over widely spread networks. This will increase the impact of data leakage. Advanced security attacks have ability to penetrate victim's network locally and then move to wider corporate network using system vulnerabilities. Therefore to limit this potential damage it is highly important to limit the advancements made by hackers in wireless LAN. Thus it is extremely important to design and implement technologies and methods to detect presence of RAPs.

1.2 Wireless Networks

Wireless networking has simplified the network setup and installation time of administrator, but has increased the security threats. Unauthorized access to the wireless network is easier than wired networks. This access can be for extending the services available on the existing network; to access any confidential information or to tamper the data flowing on the network. As the administrator is unaware of this access point, it is called unauthorized access point or RAP. Nowadays access points are very cheap and tiny so hiding them physically is very easy.

A large portion of the wireless access points and wireless network cards in the business now give up to 54MB or 108MB information transmission speed. The wireless cards and access points can produce a superb signal with their built-in antenna. The utilization of an outer antenna can further enhance the indicator quality.

The wireless access point of a system is exchanged by a malevolent access point, and the identity of the legitimate user can effortlessly be traded off. It might permit attacker to overtake the identity of true client and unite it with system.

Wireless networks are growing day by day due to their inherent advantages like less setup time, less maintenance and flexibility. The network administrator does not have to look after the network problems like wire breakages, connectivity etc. But the major problem the network administrator has to face in case of wireless network is its security. As the medium of communication is air and every communication is a broadcast communication, everybody who gets hooked to the network will get access to all the information floating in the network and can steal the information, misuse the information, corrupt or alter the information.

Wireless access points are easier to install within a small time. Once access point is installed everyone can connect through it to the existing network and get access to all the information floating on the network and can send own information on the network as well [43].

1.3 Wireless LAN

Wireless LANs create a network in which all network devices and computing devices are connected to each other by wireless medium. This wireless medium uses high frequencies. High frequency radio signals are usually used by wireless LANs for physical layer communication which offers excellent connectivity and high bandwidth. Wireless LANs are also known as IEEE 802.11. Their popularity is increasing as the medium of communication is air, there is flexibility, and ease in deployment, management and administration. WLANs are growing day by day at homes as well as enterprises because of productivity and popularity of IEEE 802.11 standards. As smart phones are widely used everywhere such as offices, hotels, airports, schools which creates a synergy effect on WLANs.

Wireless LAN standards specify two basic modes of operations. They are infrastructure mode and ad-hoc mode. In Infrastructure mode wireless networking bridges joins a wireless network to a wired network using access point. The infrastructure mode uses access point to communicate between wired and wireless devices. The access point and all local wireless clients must be configured to use the same SSID. Infrastructure mode networks advantage is centralized security management and scalability.

In ad-hoc mode, all the entities are considered as nodes. The ad - hoc mode may be adverted to as independent mode. All stations communicate peer to peer (P2P). A wireless ad-hoc network, is also called IBSS - Independent Basic Service Set. It is a computer network in which the communication links are wireless. The network is ad-hoc because each node is keen to forward data to other nodes dynamically based on the network connectivity. This is in contrast to older network technologies in which designated nodes such as routers, switches, hubs, and firewalls, perform the task of sending the data.

Stations in ad-hoc mode and infrastructure mode, both participate in their concerned networks, which are ad-hoc network and infrastructure network, respectively. The interface of a client or AP contains a radio and an antenna. IEEE 802.11 specifies groups of frequencies that may be used by a network to evade the interference with the network.

1.3.1 Wireless LAN Sniffing

Sniffing is the process in which a sniffer captures wireless LAN data packet. It is usually done when one station sends data to another station over the channel. Sniffing can be conducted by two different methods: -

1. Active sniffing
2. Passive sniffing

In active sniffing the sniffer captures the packet from all available channels. Whenever a new channel come into range, active sniffer will sniff from that channel.

In passive sniffing the sniffer sniffs packets only from specified network interface or specified channel.

1.4 Analyzing Wi-Fi Network Traffic

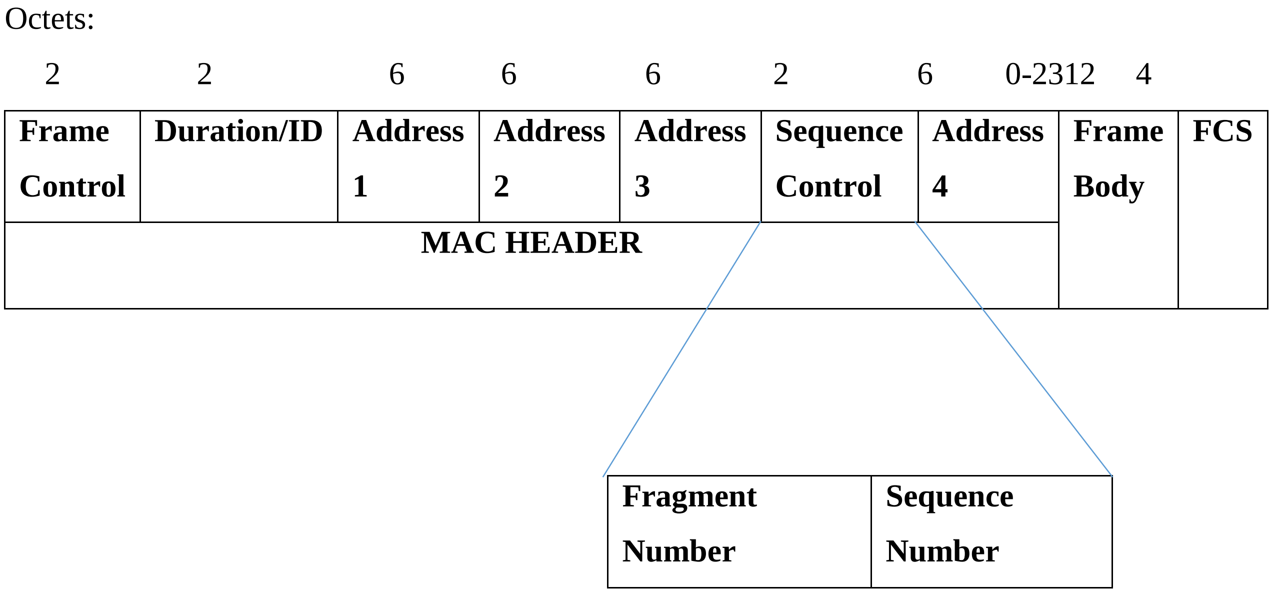
Analysis of network traffic is done using headers. Figure 1.2 shows MAC frame format. MAC frame format is used by all packets in Wi-Fi networks. Frame control field specifies which type of payload MAC frame should be transported.

Three main types of frame are given below.

- **Data Frames** – Protocol data is carried by data frames.
- **Control Frames** – RTS, CTS, ACK etc.

  RTS (Request to send) when source wants to send data to the destination. CTS (Clear to send) when the destination is ready to receive data.

- **Management Frames** –Association, Authentication, Beacon, Probe, De-authentication.



Octets:

2	2	6	6	6	2	6	0-2312	4
Frame Control	**Duration/ID**	**Address 1**	**Address 2**	**Address 3**	**Sequence Control**	**Address 4**	**Frame Body**	**FCS**
MAC HEADER								

Fragment Number	**Sequence Number**

Figure 1.2: Basic WLAN MAC Frame Format

Figure 1.2 shows basic WLAN frame sequence number which contains two bytes for sequence control fields, 12 bits for a sequence number and four bits for a fragment number.

When data or management frames need to be fragmented they are transmitted in parts with a constant sequence number and incrementing fragment numbers for each part of the packet. Figure 1.3 illustrates the basic protocol flow.

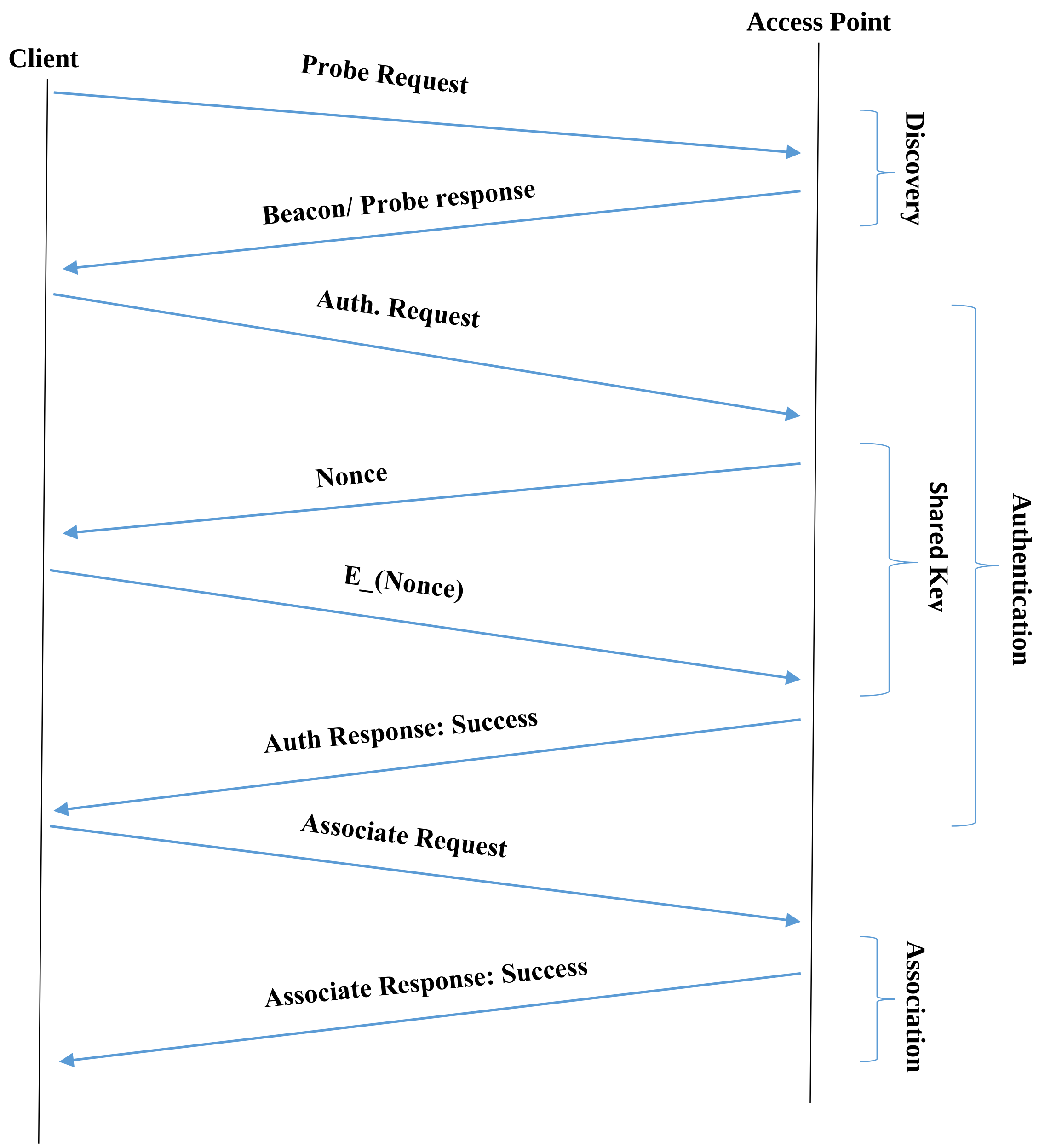


Figure 1.3: Flow of Frames

Firstly, client sends probe requests and receives the probe response to detect APs or check beacon frame broadcasted by an AP. Upon detection, client tries to authenticate the AP. If AP is successfully authenticated, then client may try to associate with the AP by sending an association request. The client will receive a positive association response if permitted by the AP. Real authentication is performed after both association and open system authentication is used [13].

1.5 An Ideal Secure Wireless System

Below are the components of an ideal secure wireless system.

1.5.1 Wireless Security Policy:

Wireless LAN is a complex system with several hardware and software technologies involved in building it. This system is used by number of people and these people work in different organizational units. These users have different access privileges while using wireless LAN. Hence it is important to create a wireless security policy that will decide what is allowed and what is not allowed. This policy can be implemented as per user privileges. This will help in securing wireless LAN by avoiding many issues that may arise because of policy violations.

1.5.2 Wireless Risk Assessment:

Before implementing any wireless security technology, a proper risk assessment of wireless network should be made. This risk assessment can be done by using vulnerability analysis and penetration testing services. Such risk assessment helps in designing appropriate security policy and deploying security technologies.

1.5.3 Wireless and Wired Architecture:

In many organizations wired and wireless networks co-exist. In such networks, there is a threat that any vulnerability in one network can result into wider losses by spreading of vulnerability across networks. Generally wired networks are faster as compared to wireless networks and traffic characteristics of wired and wireless networks differ from each other. By carefully designing the separation of wired and wireless networks many security threats can be avoided.

1.5.4 User Separation:

Many security issues arise because security policy violations take place at user level. Users have access to different objects in IT infrastructure. By using LDAP (Light Weight Directory Access Protocol) implementations available on various operating system platforms, user level access privilege can be managed effectively. This will restrict security policy violations and will also help in reducing IT vulnerabilities.

1.5.5 Authentication:

In any organization there are many standalone as well as web based applications. These applications are deployed on various operating systems. Users should authenticate themselves before seeking access to any application or operating system platform [14].

1.6 Wireless Security Threats and Vulnerabilities

Denial of Service (DoS) and distributed denial of service attack (DDoS) are two major attacks that can be launched using wireless LANs.

In DoS attacks heavy traffic is sent to authorized server using various methods. This heavy traffic makes it difficult for authorized server to conduct regular work. Thus if an attacker gains access to wireless LAN using RAPs, it is possible for the attacker to launch any DoS attack. Thus to improve wireless security, it is important to detect and remove RAP.

1.6.1 Man in Middle Attack

Man in Middle Attack is an attack in which an attacker manages to capture traffic that is being sent from one wireless client to another. This captured traffic can be copied or modified before being sent to original receiver. This attack also becomes possible because of presence of RAPs. Hence detection and removal of RAPs is necessary.

As shown in figure 1.4 an attacker can configure network deployment to implement Man- In- The-Middle (MITM) attack on any client. Here an attacker deploys a RAP and then ensures that client instead of connecting to original device, connects to newly deployed RAP. To implement it attacker can use various techniques so that client's connection will be changed. This connection can later be used for stealing important information.

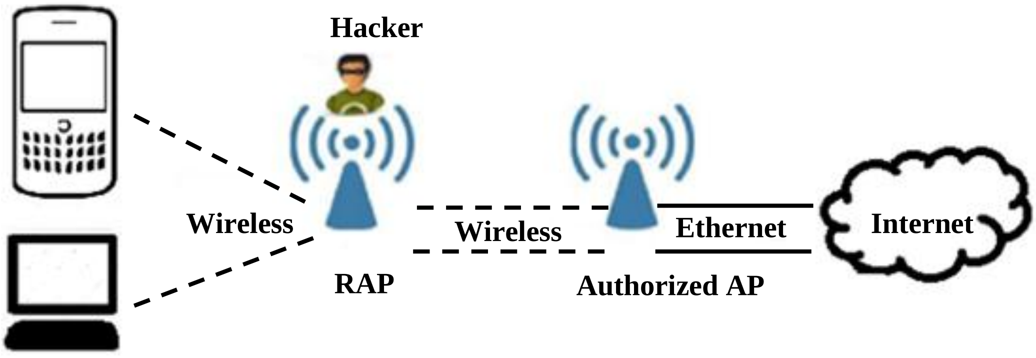


Figure 1.4: Man-In-The-Middle Attack Scenario

People have the misconception that if a firewall is present in the network then they do not need to concern about RAPs but it is technically wrong. The firewall works in between LAN and WAN networks. If an attacker creates a RAP within LAN then firewall does not detect the RAP. Even WPA2 (Wi-Fi Protected Access version 2) cannot protect a network from RAP. The security controls such as WPA2 can be installed only on managed or authorized AP. RAP is the unmanaged AP so we cannot enforce security control to it. RAP threats work at a layer below wired IDS and antivirus.

1.6.2 Eavesdropping

Wireless signals pass through air and reach any location. So it is very easy to track the radio frequency signals which is called passive eavesdropping. It monitors and analyzes the data traffic in real time. Due to antenna, range of AP wireless transmission is limited to certain distance.

1.6.3 Manipulation

In this attack type intruder can modify the data packets while sending it to the victim. For installation of RAP into the wireless LAN, an intruder can collect significant information. In active eavesdropping the RAP looks like a genuine access point where large number of clients are willing to connect to the wireless AP with a decent signal strength. All the communication can easily be tracked through RAP. If the network is open and not password protected, then the attacker can easily access the WLAN. Even if the Wi-Fi network is protected with WEP, WPA, WPA-2, attacker can easily perform various attacks using different war driving tools.

1.6.4 WLAN MAC Address Spoofing

MAC address spoofing is often used by network attacker during an attack on IEEE 802.11. This is because usually IT assets, applications and objects are protected by implementing access control list (ACL) using MAC address. These ACLs can be implemented on windows as well as Linux platforms. Hence attackers use MAC address spoofing. Thus from wireless security point of view detection of such spoofed RAP is essential.

1.6.5 Access Control List Bypassing

ACL bypassing can be performed by an attacker to gain access to internal organization network. By spoofing authorized MAC address an attacker can bypass access control lists. By conducting active and passive sniffing an attacker can obtain list of authorized MAC IDs. This list later can be used for MAC ID spoofing.

1.6.6 Authorized User Credentials

Only getting access to wireless LANs is not sufficient as most of the organizational crucial data resides inside applications that run over these wireless LANs. An attacker can use application vulnerabilities and can run exploits that will use access credentials of authorized user to gain access to application. Thus, it is clear that RAPs play crucial role in organizational data security.

1.6.7 Wired Equivalent Privacy (WEP)

As wireless LANs are prone to attackers which results into loss of privacy, WEP technology is used to protect privacy of WLAN users. Using WEP, wireless station has pre-shared key among them, and data sent over the channel is encrypted using the pre-shared key. As an attacker will not have pre-shared key, he will not be able to decrypt captured data packets. However, by capturing data packets it is possible for an attacker to determine pre-shared key, if the key is weak.

1.6.8 Wi-Fi Protected Access 2 (WPA-2)

WPA algorithm has been designed to improve security of IEEE 802.11 LANs by removing existing vulnerabilities of WEP and WPA. It removes those vulnerabilities by implementing strong encryption and authentication technologies. Encryption protects from loss of privacy, whereas authentication protects from loss of identity. To strengthen encryption, it uses AES algorithm. To strengthen authentication, it uses two methods namely, pre-shared key and IEEE 802.11 standard authentication. Pre shared key is initially used in normal mode whereas later it is used in enterprise mode. This improved security removes existing vulnerabilities.

1.6.8.1 Vulnerabilities of WPA2

Although WPA 2 is improved version it still has plenty of vulnerabilities. Some existing vulnerabilities of WPA2 are discussed below [22].

- IEEE 802.11 standard is mostly defined at data link layer and leaves physical layer security to be handled by other technologies. This makes WPA 2 vulnerable to various physical layer attacks that could result into loss of availability.
- Various frames are used during working of wireless LAN, which are responsible for successful configuration and deployment of wireless LAN. These frames are vulnerable to various attacks and could reveal sensitive information to attacker about networks system details.
- WPA 2 asks its users to deauthenticate, so as to improve security but this feature could be misused by an attacker to implement various spoofing attacks.
- WPA2 also has feature called disassociation which could also be misused by attacker to launch various authentication attacks.

1.7 Rogue Access Point

Rogue access points are malicious access points deployed in IEEE 802.11 based wireless LANs without any authentication. Generally these devices are added to gain unauthorized access to wireless LAN. The RAP gives authorization to attacker to conduct MITM attacks. The existence of such RAP causes immense security threats in a wireless LAN.

Once attacker manages to install his access point inside wireless LAN, it will work as an authorized access point and an attacker will be able to execute various vulnerability detecting applications on host wireless LAN. These detected vulnerabilities can then be exploited by using various exploits.

Given below is the list of possible attacks that can be launched on host wireless networks using RAPs.

- As host network can be connected to wired network and an attacker can intrude inside wired network.
- An attacker can obtain the details of entire network.
- An attacker can also obtain details of individual hosts on wireless LANs.
- Data over network can be sniffed.

Most of the firewall work is at transport layer and hence cannot detect the presence of RAP. Authorized access points use encryption protocols like WEP and WPA2 but are not able to provide all security measures. Hence encryption, anti-virus, firewall all fail to detect the presence of RAPs.

Moreover, many RAPs copy beacon frames are sent from authorized access points and hence it is easier for them to bypass any authentication mechanism that is present to authenticate access points.

Many attackers manage to remove the authorized access point from wireless network and successfully plant their access point as authorized one. Such type of attack is more dangerous to an organization's security. Most of these RAPs are deployed by internal employees and hence are difficult to detect.

One of the major vulnerabilities that WLANs face is the misuse of access points, also known as RAP as shown in figure 1.5. Without permission of network administration RAP devices are deployed in secured WLANs. The bearing of such RAP causes severe threats to the WLAN security.

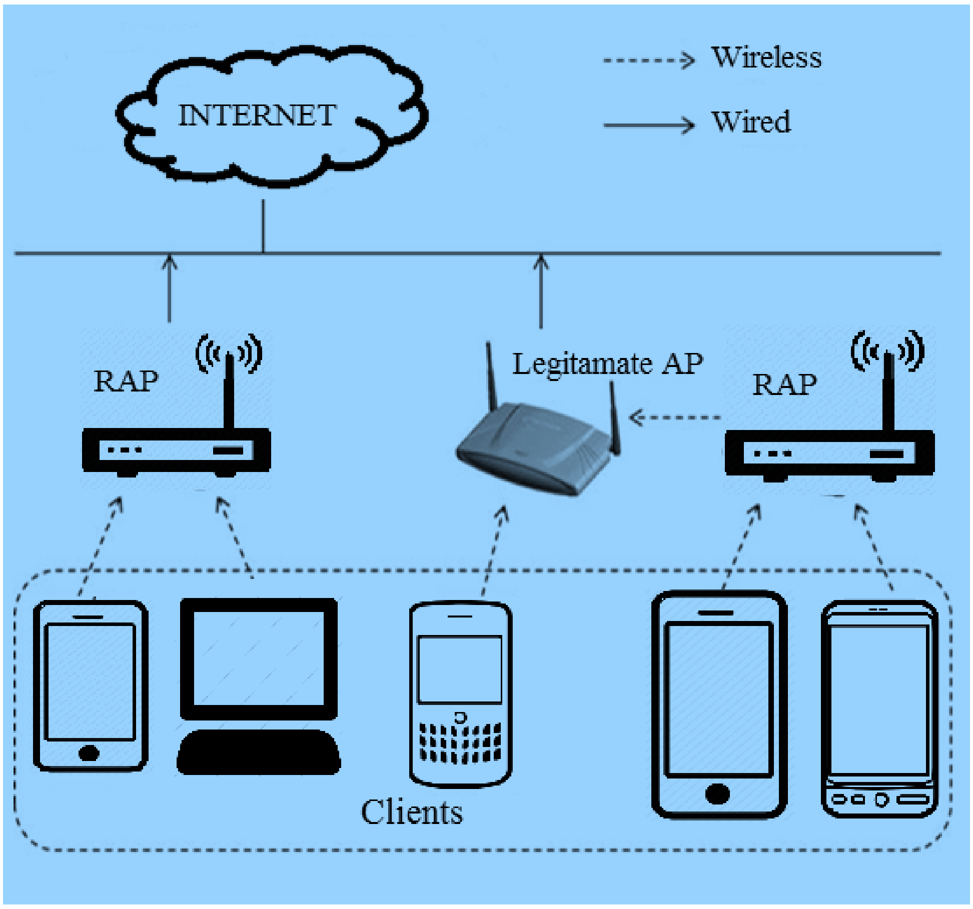


Figure 1.5: Rogue Access Point

Security threats in WLANs are rapidly evolving because of the variety of attacks in wireless technologies. Client's confidential information such as bank account details, credit card number, e-mails can be hacked by attacker if they use internet services through AP or smart devices. It is very important to determine whether connected AP is authorized or RAP because attacker can easily perform MITM attack to steal the confidential data and disturb network service.

RAPs are major security threats because they are not secured. Malicious attacker in the neighborhood can effortlessly connect to the internal network through these RAPs, evading all security measures. The effects of RAPs are visible for both wired and wireless side of the network.

There are different types of RAPs like unauthorized, improperly configured, phishing and compromised APs.

- Unauthorized Access Point: There are instances when an employee himself installed the AP in such a way that the web administrator is not aware of it. This is performed in order to acquire flexibility, scalability and to sniff data and bandwidth.
- Improperly configured Access Point: Access point configuration settings include such as IP address, radio channel, data rate, beacon interval. If any one of these settings is not done properly then access point can easily become RAP.
- Phishing Access Point: If an unauthorized user installs an AP in order to obtain user's credentials like usernames and passwords by masquerading as an authorized user, it is termed as phishing access point.
- Compromised Access Point: In this the attackers are able to crack the key that is used in WEP and WPA PSK enabled network. If an attacker finds out the key, then all the APs that are using same credentials are also compromised and this results into a RAP.

1.8 Necessity for Rouge Access Point Detection

There are four major types of losses that result after a network security attack. These losses are listed below:

- Loss of confidentiality
- Loss of availability
- Loss of integrity
- Loss of identity

In loss of confidentiality the contents of the IT objects are seen by unauthorized person resulting into loss of confidentiality.

Many times attackers launch an attack on server and ensure that the server will not be able to function properly. When this happens, authorized clients will not be able to get any service from the server. Such kind of loss is called as loss of availability.

There are some attacks where an attacker obtains the data, when data is being transferred over channel. This midway obtained data is then modified by an attacker. An attacker then sends this modified data to original receiver. For this receiver there is no way to know whether data has been modified or not. This kind of loss is called loss of integrity.

In some attacks an attacker uses identity of some other user or computer and sends message to authorized user. This makes authorized user to make wrong conclusion about sender's identity. Such kind of loss is called as loss of identity.

Whenever RAP is deployed in IEEE 802.11 wireless LAN, an attacker can launch various attacks that will result into all major losses that are mentioned above. Moreover, if wireless LAN is connected to wired LAN, then there is possibility of an attacker gaining access to inner part of organization network. Looking at these losses it can be definitely concluded that presence of RAP is a major threat for organizational security. Therefore, there is need to develop technologies and methods to detect the presence of RAP.

1.9 Types of Rouge Access Points

To detect presence of RAPs first it is necessary to describe and identify which access point can be called as RAP. Below is the list of RAP types:

- Employee's RAP.
- An attacker's external RAP.
- An attacker's internal RAP.
- Neighborhood RAP.

Employee's RAP:

Wireless access points are commodity and employees can buy and obtain them very easily. In many organizations there is absence of wireless/wired network security policy. Many organizations do not even have any LDAP based authentication technology implemented. In such cases, it is possible for the internal employees to bring their own wireless access point in office premises and deploy them without any authentication. This type of unauthorized wireless access point is termed as employees RAP.

Attacker's External RAP:

An IEEE 802.11 wireless LAN uses radio frequency in high frequency spectrum. Due to reasonably large area covered by these frequencies, it is possible for a wireless access point to cover area that is outside the office premise. An attacker can then deploy his RAP outside office premise and still get connected to authorized wireless access point. This type of external access point is called as attacker's external RAP.

Attacker's Internal RAP:

Sometimes an attacker can manage to get an access to internal organization network physically. This physical access would give him an ability to deploy unauthorized access point within office premise. These access points are called attacker's internal RAPs.

Neighborhood RAP:

IEEE 802.11 wireless LAN uses unlicensed frequency band. There is possibility that wireless access points deployed by other people are visible in nearby places. In this case organization do not have control over the wireless access point and employee's from office may get connected to other wireless access points unknowingly. These neighborhood access point can also be called as RAP.

1.10 Methods of Detecting Rogue Access Point

1. IT persons are equipped with wireless packet analyzer tool on their handheld device and they can move through the campus to search access point [22].
2. Checking the radio frequencies using some sensors placed at different locations in the campus, as the access points broadcast beacon frames containing SSID at regular intervals. So by capturing such frames user can identify the presence of the access point [9].
3. Checking the IP traffic on the network. If two consecutive packets are sent on the network, then the packets inter-departure time on wireless network is more than wired networks [14].
4. Run a port scan on the network looking for port 80 (HTTP) interfaces, which includes all web servers, printers and all access points. Though an access point's port 80 interface is disabled or protected with a password, the device

will usually reply to a request for some basic information that may be useful in determining its status [11].

5. Measuring Round Trip Time (RTT) of the packet send on the network. This is done by sending a packet to the known host on the network and calculating time when the reply of the packet is received. If the round trip time is significantly longer, it means that there exists a wireless network [13].
6. By listening the airwaves RAPs can be discovered. Different software and hardware products available in the market make this possible [38][39].
7. NetStumbler [34] sniffer software allows to carry a laptop around the network, which scans all radio frequency signals of all access points. It is very time consuming to walk through all of the network in search of rogues.
8. It must be determined whether the discovered unrecognized access points are rogue. This type of RF audit is costly, incomplete, and too intermittent to continuously protect the wired network from rogues and if the network covers many geographically dispersed locations, this method of rogue detection may be unworkable [22].
9. Electronic devices can be installed for continuous vigilance of RAPs, which continuously monitor all Wi-Fi traffic within their range. This can be an expensive proposition. Not just in the cost of the probes, but also in terms of pulling ethernet cable and providing electrical power [24].
10. Most of the existing probing methods consume huge network bandwidth. When probing is used, security expert need to employ war driving method in which expert will roam throughout the wireless LAN with probing software in search of rogue device. War driving is impossible when wireless network is bigger and also it is not foolproof, as rogue device will keep itself off for the time war driver is in its range, the moment driver goes out of range rogue device will turn on itself. Legitimate access points of adjoining wireless LAN will be detected as rogue by probing method, thus generating false negatives [12].
11. Sniffing is used to capture the data over network which is effective on shared medium networks. Sniffing place an ethernet network interface to "promiscuous mode". It processes all packets on the Ethernet. NIC card gathers all packets in that particular collision domain. In switched network

environment, each switch port has its own collision domain, while all hubs in a non-switched network is a single collision domain. In sniffing proximity is a vital factor, traffic may be sniffed at any physical connection between the sender and receiver. Sniffing a client-server communication over the internet may happen using cable modem segment, leaving the client's neighborhood networks at the Internet Service Providers (ISP) connecting the cable provider to the ISP server's [15].

12. Sniffing session gathered information depends on two factors. The first is how much data was gathered. The eavesdropper will have the entire communication if the entire packets of the session are captured. A sniffer installed on a system in the path of the communication is no longer stealthy if the captured session grows largely exhausting the disk space of the server. The second factor is the eavesdroppers' ability to decode the communicated packets. Well-known services have popular decoders available. Encrypted sessions are useless to an eavesdropper unless the user can brute force the keys used to encrypt the session [15].
13. Rogue Access Point Localization - After discovering the RAPs, it is necessary to locate RAP and perform the countermeasure. The localization is the process to discover if the RAP is connecting to the company's network and to which switch port the RAP is connecting. AP localization technique relies on the sniffing data getting from the wireless client that is associated with the questioned AP. The wireless client accesses the network through the interrogated AP. The data header includes the wireless MAC address of the wireless client. If wireless MAC address of the wireless client appears at any port of the internal switch [17].

1.11 Need for Research

Traditional approach of RAP detection uses the concept of MAC address checking and wireless traffic analysis. Nowadays attacker can easily overcome challenges of traditional approaches. Many commercial software tools like Airtight [32] WIPS, Aerohived are available for detection of RAP in networks.

RAP detection can be broadly classified into two different approaches, Client side approach and Server side approach. The server side approach is further divided into two parts viz. centralized and decentralized approaches. Some techniques use a hybrid approach. In server side approach software tool is installed on the central node, basically called the server which handles the whole network and detects RAP. The client side approach is challenging because there is no former information about network, to act as reference. Even client does not know about the authorized access point list and nodes do not have any sophisticated software tool available within it.

Industrial and academic researchers, both are working on this issue to find a better solution for detection of RAP [6].

1.12 Motivation

In previous researches, a number of solutions were provided for RAP detection. There are two RAP detection methods: server side and client side. In existing RAP detection methods server side approach uses centralized node basically called as a Wireless Intrusion Detection System (WIDS) node. It can monitor the network for the detection of RAP. It uses authorized AP list, clock skew of AP, standard encryption and authorization technique, sequential hypothesis test. The major drawback with the server side approach is if the central server is not available or compromised then the system will not work properly. If client node is within the reach of a server then it can provide service to client, i.e. the mobility of the service cannot be provided by the server. The server side approach is expensive, limited and does not work for many scenarios.

The client side approach provides mobility to the node about service. It uses a technique like timing based scheme, bottleneck bandwidth analysis, received signal strength, inter-packet arrival time. But practically these methods are cumbersome process for detecting RAP. From these limitations of existing solutions it was understood that there is a need to consider additional parameters. This acted as a motivation to design a new method that considers multiple parameters for RAP detection.

1.13 Problem Statement

To Develop an Efficient Technique for Rogue Access Point Detection Using Multiple Parameters.

1.14 Objectives

1) To study the existing methods of RAP detection for WLAN.
2) To design and implement effective RAP detection algorithm for WLAN.

3) To analyze and compare the performance of developed RAP detection algorithm with existing methods for RAP detection for WLAN.

1.15 Organization of Thesis

This thesis contains the description of method used for successful detection of presence of RAP in authorized wireless LAN i.e. IEEE 802.11.

This thesis has been structured in to various chapters as follows.

Chapter 1:

In this chapter, Wireless network, Wireless LAN, RAP, its types and WLAN security issues are described. It describes motivation, problem statement, objectives and research issues.

Chapter 2:

This chapter covers a detail literature survey of existing methods. It also explains industry and academic researchers' solution for RAP detection. Existing techniques and their drawbacks for detecting presence of RAP have been described.

Chapter 3:

This chapter explains how different RAP detection techniques are implemented. The advantages as well as disadvantages of these implementation are studied from the experimental results and analysis.

Chapter 4:

This chapter explains the multi parameter based method used for RAP detection. This description contains mathematical model, algorithm and architecture of multi parameter method.

Chapter 5:

This chapter lists experimental findings and analysis of the multi parameter based method. The findings describe RAP detection test cases using various parameters such as SSID, MAC, frequency, signal strength, timestamp and sequence count. The results are analyzed using confusion matrix. It also discusses result and findings obtained after various experiments. This discussion analyzes findings with respect to research objectives.

Chapter 6:

This chapter concludes the thesis findings and describes the future scope.

CHAPTER-2

LITERATURE REVIEW

This section reviews the work done in the area of wireless LAN security and RAP detection methods by the researchers from both the industry as well as the research institutes in the world. The related work, published in the standard international journals; proceedings of international and national conferences; various articles related to international symposiums and workshops were referred for this work. The work which is available in standard books and websites were referred. Based on the research work carried out, limitations of existing methodologies related to WLAN security have been traced. This has led to the motivation for the development of multiparameter based RAP detection method.

2.1 Academic Researcher Solutions

Yang et. al. [1] have proposed client side Evil Twin detection technique. This technique presents two algorithms: Training Mean Matching (TMM) and Hop Differentiating Technique (HDT). These algorithms use Inter-Packet Arrival Time (IAT) to detect Evil Twin AP. This technique does not need authorized AP list and it does not rely on training data or types of wireless network. The major problem with this technique is that it cannot work for all kinds of MITM attacks in the wireless networks. This technique may not work properly if remote servers are not available.

Kao et. al. [2] have proposed client side RAP technique using bottleneck bandwidth analysis. It uses a passive packet analysis approach. It is based on bandwidth estimation using pair technology. They also proposed another approach called as client side bottleneck bandwidth with sliding window to get better accuracy with detection technique. But this technique has a problem of reducing the size of the sliding window. Packet analysis requires a sophisticated algorithm design which can be quickly deployed to protect the entire network.

Kim et. al. [3] have mentioned client side approach using the concept of received signal strength (RSS) for RAP. In this method they find highly correlated RSS sequences which can be collected in the wireless device. Sequential hypothesis technique is used to normalize the received signal and classify whether the collected signal is multiple or not. It is a lightweight solution to overcome the drawbacks of the client side approach. This technique does not consider the distance between the client node and access points while calculating the signal strength, although distance affects the signal strength.

Liran Ma et. al. [4] have proposed a hybrid approach which contains a model for RAP detection that includes packet collector, unauthorized access point preemption engine and detection engine. This system provides a cost effective solution. This model follows the traditional approach for RAP detection which has many pitfalls. In this paper, author tend to provide a comprehensive taxonomy of rapscallion APs. Classification includes improperly designed APs, phishing APs, unauthorized APs, and a replacement category of rapscallion AP termed as compromised APs. Authors have developed a completely unique system for shielding commodity Wi-Fi networks from rapscallion APs known as RAP.

Shivraj et. al. [5] introduce a server side Hidden Markov Model (HMM) based approach to detect RAP. This method uses variation in packet inter arrival time to differentiate between authorized access point and RAP. It provides average detection accuracy up to 85%. It is easy to manage and maintain. It requires minimal effort and deployment cost. This new approach achieved variations in packet inter arrival time to get authorized access points from RAPs. This proposed model can detect the presence of a RAP promptly within one second with exact accuracy i.e it has very low false positive and false negative ratios .But this technique requires too many trained data for detection and also it works for only specified Denial of Service attack.

S. Nikbakhsh et al. [6] have proposed a new method for detecting man in middle attack and evil-twin attacks. These attacks are generated by RAP and in this method data collected at routers and gateways is used to detect these attack signatures. The main benefit of this method is it can be easily deployed over any network.

Jana and Kasara [7] have proposed a novel solution in which clock skew values are used to detect RAPs. A clock skew is an important parameter that every access point has. Access points with beacon frames can be easily differentiated by analyzing their clock skew values. This analysis can be further used to detect RAPs. Traffic characteristics of wired network and wireless networks are different where wired networks are fast as compared to wireless networks. Clock skews act as fingerprint, and hence, are unique to each access point.

Kindberg et. al. [8] have proposed server side model which provides security to public Wi-Fi network. This model uses standard encryption and authentication technique with some modifications. This method allows the authorized user to authenticate the access point in a wireless network.

Bo Yan et.al. [9] have proposed a solution in which a verifier is developed that detect the RAP by processing information obtained from wireless sniffer. This method also works with congested wireless networks.

Roth et.al. [10] have proposed a solution to detect evil twin attacks generated by RAPs. This method also implements host authentication using key exchange cryptography. Thus authentication and detection of evil twin attacks improves wireless security.

Han et. al. [11] have proposed timing based scheme for RAP detection. It uses a client side approach where the emphasis is on Round Trip Time (RTT) between the user and the DNS server to check whether the access point is RAP or not. This paper considers a class of RAPs that pretend to be legitimate APs to lure users to connect with them. Authors tends to propose a sensible timing-based technique that permits the user to avoid connecting to RAPs. Author tend to enforce the detection technique on commercially obtainable wireless cards to gauge their performance. At constant time, the detection solely needs less than one second for lightly-loaded traffic conditions and tens of seconds for significant traffic conditions. While existing techniques will alleviate this threat, they yet require active participation on the part of the network administrator. The detection algorithm is effective and accurate but it considers only wireless traffic between the station and the tested AP. The case of multiple RAPs colliding with each other is not considered in this method.

Songrit Srilasak et. al. [12] have proposed combined solution for finding and counter attacking the RAPs. Access point in the central system collects wireless data. It also performs classification of RAP and analyzes related risk assessment. RAP can be detected by analyzing the wireless data. After analyzing the data if RAP is found then the port is disabled by using central system. The system uses existing access point as the wireless sensor, hence no dedicated wireless sensor is required. The solution is effective, low cost and also works on existing wireless infrastructure. As central system takes the wireless data from RAP, if it goes down then the whole system will collapse. Therefore proper wireless security policies are needed.

Shetty Sachin et. al. [13] have proposed a RAP detection technique using network traffic characteristics. Here unique approach is proposed to detect RAP having wired and wireless networks. This approach is applied in two successive phases. A network traffic analyzer (NTA) is used to analyze traffic gathered at the gateway router. NTA analyzes the traffic on WLANs to calculate the frequency of straight and crossings access attempt. Access attempts frequency exceed a threshold, then NTA will alert the network administrator that end-host is connected to RAP. The main idea of this work is to separate authorized WLAN hosts from unauthorized WLAN hosts connected to RAPs by analyzing traffic characteristics at the edge of a network.

Beyah, R. Kangude, et. al. [14] have proposed a scalable solution that uses temporal traffic characteristics to detect RAP independent of the signal range of RAPs. It compares traffic characteristics of different wireless APs. The detection given in this paper is independent of the wireless technology like 802.11a, 802.11b, or 802.11g. It is possible to potentially perform RAP identification using inter-packet spacing without need of human intervention.

Han et. al. [15] have proposed a network based intrusion detection with data mining, to learn signatures. Network behavior patterns is used for detecting malicious attacks which goes undetected. Hence, this system monitors and learns about normal network behavior. Network Attack Detection System (NADS) uses both signature and anomaly-based techniques. It alerts security administrator when NADS detects an intruder. It is a relentless effort to detect the presence of network attacks.

P. Bahl, et. al. [16] have developed a framework which monitors wireless networks of enterprises using desktop infrastructure, called Dense Array of Inexpensive Radios

(DAIR). It demonstrates that the DAIR framework is useful for detecting rogue wireless devices attached to corporate networks, as well as for detecting Denial of Service attacks on Wi-Fi networks. There are some attacks that network administrators of corporate Wi-Fi networks have to guard against. These attacks are broadly classified as passive and active. The classification is important to understand the strengths and limitations of the DAIR security management system.

H. Yin et. al. [17] have developed architecture for layer 3 RAP detection. If wireless sniffer picks up special packets, then it is confirmed that the suspected AP that relays these packets is RAP. There are two issues for robust detection.

1. Using NAT (Network A ddress Translation) module multiple devices can share the same connection and hence it is not possible to send test packets directly to the associated wireless clients, because they have private IP addresses in wired side. The new outbound packets have their own address and to send test packets to the active sources it uses the verifier. The test packets will be forwarded by NAT and are captured by wireless sniffers, if an active source is an AP

2. If the AP has enabled encryption then sniffers may not be able to recognize test packets by examining the payload. A probabilistic verification algorithm is devised based on a sequence of packets of specific sizes.

Lanier et.al. [18] have proposed a method which uses Round Trip Time (RTT) of network traffic to distinguish between wired and wireless nodes. It uses the lower and higher value change RTT in a wireless network. Authors have shown that the lower capacity of the wireless nodes have greater RTT associated with their packets. As the capacity of wireless links increase it is likely that the RTT associated with the wireless link will come close to that of the current wired links. However, as the capacity of the wireless link increases so will that of the wired links. This information coupled with a list of authorized APs allows to detect RAPs one hop away from the offender.

M. Tung et. al. [19] have proposed the RAP Detection and Localization (RAPDL) architecture combined into one system. This is client-server based approach. First client will collect the information about RAP, and its properties, then send this collected information to the server. After receiving AP data from client, server will execute the localization algorithms to detect and find location of RAPs. Two localization algorithm have been followed here, one is distance-based and another is fingerprint-based algorithm.

V. S. Shankar et.al. [20] have proposed a technique which uses mobile Multi-Agents for spotting and removing RAPs. Authors have projected a novel method of exploiting Multi- Agent as associate degree integrated resolution for each detective work and eliminating the scallywag access points from the network. It uses master and slave mobile agents. To regulate the authentication process master mobile agent is used for generating slave agents, which are then transmitted to the corresponding APs. Now these slave agents are replicated on every AP, and transmitted to every connected client system. The duplicated slave agent sends the information packet details of the unauthorized AP to duplicate agent to the connected AP when it detects new access point. The slave agent reports the information to its master agent on the server. So the suspected AP is detected and matched with the previous stored information about the APs. If the information is matched then it generates a new slave agent and send it to that AP, else the port at which the MAC Address is connected is examined and blocked. Authors tend to propose a Multi-Agent Based Methodology that not only detects RAP but conjointly fully eliminates it. This technique has the following outstanding properties: (1) Any specialized hardware is not required (2) the proposed formula detects and eliminates the RAPs from network (3) Solution is cost effective. This multi agent based design does not solely identify and eliminate the scallywag access points fully.

Wei et. al. [21] have proposed two online algorithms which utilize sequential hypothesis test for unauthorized AP detection. Router traffic is monitored to take a decision about TCP-ACK pairs. Drawback of this method is that it depends on data gathered at router and switches which can change.

Raheem Beyah et. al. **[**22**]** have proposed a method which block back door rogue devices. Since APs have reached commodity pricing, the demand of deploying them in an unauthorized fashion has grown. Also, because APs have become considerably smaller, network administrators have difficulty in visually detecting them. This is particularly true if an attacker uses a laptop as an AP. Unlike traditional attacks, which initiate outside the network, RAP insertion is most often due to inside users. This can have significant consequences because these rogue devices create a back door to the network and threaten network security.

Jie Yang et. al. [23] use physical property spatial information which is hard to falsify. Cluster based mechanisms are developed to determine the number of attackers. It detects wireless spoofing attacks and determine number of attackers and adversaries.

Sia Sie Tung et.al. [24] have proposed wireless security in the physical layer, dealing specifically with Access Points (AP). Beginning with the physical layer the importance of layer one security must not be taken too gently. Good access points are a main issue to attain decent security for the wireless network. Author do not want high-ticket, high-end access points to stay secure. Easy defensive methodologies should always be taken into account, such as SSID and protocol filtering.

Donald R. Reising et.al. [25] have implemented a method in which unauthorized network access and spoofing attacks at wireless access points (WAPs) are historically addressed as victimization bit-centric security measures and stay a major data technology security concern. This has recently addressed victimization RF process strategies among the physical layer to enhance WAP security. This paper extends the RF process knowledge domain by: 1) Distinguishing and removing less-relevant options through dimensional reduction analysis (DRA) 2) Providing a primary look assessment of device identification (ID) verification that allows the detection of scallywag devices making an attempt to achieve network access by presenting false bit-level credentials of licensed devices.

Thambo Nyathi et.al. [26] have proposed a system that uses dynamic value to produce time. Due to latency of the beacon frame values y and y' changes. If repeaters are used between the clients and AP difference is likely to increase. Due to latency scalability is likely to suffer. Clients can be stopped from connecting to unauthorized access points by manipulating the beacon frame. Using free bits of any information element beacon frame can be manipulated.

Hao Han, et.al. [27] have considered vehicular RAPs the APs area discovered in moving vehicles to mimic legitimate margin APs to lure users to associate to them. Due to its quality, a conveyance RAP is in a position to keep up an extended connection with users. Thus, the opposer has to wait long to launch numerous attacks to steal users' personal info.

Jonny Milliken, et.al. [28] present a new approach of detection strategy for the chameleon Wi-Fi AP virus. Proposed system uses two algorithm, first is dynamic outer detection and another is AP traffic identity detection which helps to attribute identity to specific AP from collection location. This approach represents new type of AP attack which is considered as more advanced and difficult to detect. Research provides various security solutions such as user privacy and user confidentiality while detecting attacks.

Sartid Vongpradhip et.al. [29] present a new approach distributed intrusion detection system (DIDS) to handle attacks on network and survive it by making the use of mobile agent technology with the network topology design. It hides main resource of the network in the back of IDS, which divides network resource into segments and also installs the monitored host on each network segment. This results into robustness from all types of attacks. The research provides various security solutions such as the design to avoid single point of failure. Also shadow agent together with proxy agent, provides fast backup and recovery technique, and the encryption of the communication between all the IDS and multicast groups for the network security. Architecture uses public key cryptography to reduce the cost.

Hao Han et. al. [30] have proposed a practical timing based technique which allows the user to avoid connection to rogue access points. The method presented in this paper gives the round trip time between the user and the DNS server, which determines if AP is legitimate or not without assistance from the WLAN operator. The approach presented here is implemented on commercially available hardware for evaluation. Paper represents RAP detection scheme which is implemented purely by end users. The purpose of RAP detection algorithm is based only on existing networking protocols to work and can be applied to any regular WLAN network which does not require further modifications by network administrators.

Gaogang XIE's [31] Research indicates that the experiment on an operated network shows the average detection ratio of the algorithm with STJ is more than 92.8%. The average detection time is less than 1 second with improvement of 20% and 60% over the detecting approach of ACK-Pair. Research work presents main three contributions including STJ, which can distinctly reflect wireless MAC mechanism and is used to classify wire and wireless traffic. Next is an analytic model of STJ which is deduced from the DCF Markov chain model and last is a RAP detecting algorithm which is based on the analytic model presented without training trace. Receive Signal Strength (RSS) is used to forestall users from connecting to RAPs. The ease of putting in a productive RAP in conveyance makes this way of wireless attack a very serious security downside in conveyance networks. During this paper, author is the first to demonstrate the feasibility of this kind of RAPs, and gift a sensible defensive schemes to forestall the users to attach to conveyance rogues.

2.2 Industry Solutions

Air Defense [32] provide a complete software and hardware system which contain sensors deployed throughout the network. Management console is provided to network manager to handle the tool. Starter kit can manage up to ten APs and provides five sensors. It spots malicious attackers and intruders, and also detects vulnerabilities in the network. Air Defense senses malicious attacks and intruders. The latest version can respond to intrusion attempts within a few milliseconds of the attack. Air Defense can be easily synchronized with a “honey pot” for its efficient working. The drawback of this commercial tool is that its response time is very slow to detect the RAP.

AirMagnet [33] is another commercial product which is used for detection of vulnerabilities and intrusions. It detects RAPs and Denial of Service (DoS) attacks by flooding. This software requires a technical person to move around the network for detection of security threats.

NetStumbler [34] is a popular tool available on windows platform and it works as active sniffer. Sniffer sends probe request using BSSID and captures the network traffic. It adheres IEEE 802.11 specification while conducting probes.

Kismet [35] is a sniffer which has ability to detect hidden networks and capture network packets from these hidden channels. It can also obtain information about network interfaces and protocols used. Kismet works in monitoring mode and hence cannot send packets when probing is going on.

Airsnort [36] is popular Linux tool that is used to obtain pre-shared key. Airsnort can capture data packets which are encrypted using WEP and can analyze them to determine pre-shared key. However, Airsnort cannot determine pre-shared key if it is weak. To mitigate this threat NICs are available which increase the strength of wireless LAN, WEP even in case of weak pre-shared key. However, wireless client that do not use these NICs are still vulnerable to Airsnort.

Air Snare [37] is a program for windows that detects DHCP requests or unauthorized MAC addresses attempting to connect to an AP. Intrusion response consists of an alert to the administrator and optional message is sent to the intruder via windows net message. The disadvantage of this tool is that once the main server of detection is hanged due to excessive network accesses, this tool stops working. This tool will not be more useful in case of large number of DHCP requests. For such cases one needs to use load balancing approach to handle all the requests concurrently.

Airjack [38] is another tool just like Airsnort which can be used to demonstrate various attacks on IEEE 802.11 WLAN. Airjack can demonstrate man in middle attack as well as various spoofing attacks.

2.3 Limitations of Existing Methods:

From the above literature survey following limitations of existing RAP detection methods are observed.

i) **Clock Skew Solution:** It is assumed that first, the authorized AP will be activated and then the RAP. But this assumption is weak, as one cannot control which AP will be activated first [7].

ii) **Inter Packet Arrival Time:** Can be used to detect RAPs, but it is not effective when Evil Twin is present [11].

iii) **Mobile Agent Code:** Mobile agent code is small, and is installed on a mobile device for the purpose of detecting RAP. A mobile agent code cannot be installed without client permission, which results into a major drawback of this method [29].

iv) **MAC Address and SSID:** SSID and MAC address are used to detect RAP. These properties can be spoofed by using many tools available on internet [23].

v) **RSS Level:** RSS of the access point is used by various methods to detect RAPs. But the variations in RSS levels can cause variation in results [3].

vi) **Wireless Traffic:** In wireless environment, network traffic can provide inaccurate results. Such inaccurate results create a suitable environment for RAP to perform attacks [13].

vii) **Server Side Approach:** The major drawback with the server side approach is that, if the central server is not available or compromised, then the system will not work properly. If client node is out of the reach of a server then server cannot provide service to the client. The server side approach is expensive, limited and cannot work for many real life scenarios [20].

2.4 Existing Methods for RAP Detection and Limitations

2.4.1 Brute Force Approach:

- This approach is not completely effective and it takes more time to detect RAP.
- IT personnel install wireless packet analyzer tools on laptops and scan the network traffic.
- When the scan takes place RAP can easily be unplugged.
- In order to accommodate multiple frequencies, IT personals must upgrade their detection devices.

2.4.2 Enterprise-Wide Scan from a Central Location:

- To monitor the air waves sensors are put across the network, which is expensive.
- If an attacker uses a directional antenna or reduces the signal strength to cover the small range within the office, this approach can be ineffective.

2.4.3 RF Monitoring:

- This method exploits additional information gathered at routers and switches.
- It is deeply dependent on specific features of IEEE 802.11, which can be easily turned off.

2.4.4 RAP Detection through Temporal Characteristics of Wireless Networks:

- It is mandatory for the wireless access points to be directly attached or one-hop away from the monitoring point.
- The detection is effective only when wireless hosts are uploading data.

- The approach is based on visual inspection, which makes it difficult to detect RAPs automatically.
- Inter-packet arrival times of wireless traffic are more random than those of wired traffic.

2.4.5 Detecting RAP Using Wired Approaches:

- This method detect APs by querying routers and switches for MAC address assignments.
- This solution fails because MAC address can be spoofed or cloned easily by RAP.

2.4.6 RAP Detection Using Mobile Agent:

- Mobile Agent code is installed on all authorized nodes in the network.
- But the limitation of this method is that mobile agent code cannot be installed without client's permission.

2.4.7 Network Attack Detection Using Concept of Data Mining:

- This solution is not effective because it takes more time to scan and search a signature in database using Apriori algorithm.

2.5 Summary:

The above literature survey shows that the research papers mainly discuss about the methods to detect RAP using different parameters which can be spoofed by attackers. The vulnerabilities stated above are observed in the existing methods, using which intruders perform various attacks on WLAN. From these vulnerabilities it was understood that there is a need for considering some additional parameters. This acted as a motivation to design a system that considers multiple parameters for RAP detection. The thesis thus addresses the design, development and implementation of the new method which uses multiple parameters for RAP detection, which has not been considered in the reviewed papers.

CHAPTER-3

DESIGN AND DEVELOPMENT OF RAP DETECTION TECHNIQUES

While working on the first objective of this research, which was to study the existing methods of RAP detection for WLAN, different RAP detection techniques were implemented, which are listed below:

1. RAP detection and prevention using mobile agent intelligence.
2. WLAN Evil Twin AP prevention using computational approach.
3. Elimination of fake AP in WLAN using received signal strength.
4. Illegal access point prevention in Wireless LAN using clock skews.
5. Providing data security in WLAN by detecting unauthorized access points and attacks.
6. Illegal access point detection for WI-FI network by using hybrid approach.
7. Unapproved access point elimination in WLAN using multiple agents and skew intervals.

The advantages and disadvantages of these implementations were studied from the experimental results and analysis. These limitations served as the motivation to develop a more robust solution for RAP detection.

All the above mentioned techniques are briefly discussed below.

3.1 RAP Detection and Prevention Using Mobile Agent Intelligence

An efficient Mobile Agent (MA) based RAP detection technique is proposed in this method. A mobile agent has features like local network monitoring to overcome latency in network and reducing the load on network; various autonomous and disconnected operations; asynchronous execution and adaptability of diverse networks.

The mobile agents are used to cover more area than traditional RF and SSID scanning. The total area will be divided into territories for every MA, limited to scan on their local area. Thus reducing the network overhead [29].

3.1.1 Mobile Agents

A mobile agent is a combination of a small code and data which is executed on destination computer to perform desired task. Agent can remain immobile and communicate with the environment by standard methods. The agents who do not move are known as stationary agents.

3.1.2 Experimental Setup

The system will divide the complete network into different territories and invoke the mobile agent located in that territory. These MAs will scan their respective territory and send the outcomes to the server located centrally which will then apply different policies to consider the result.

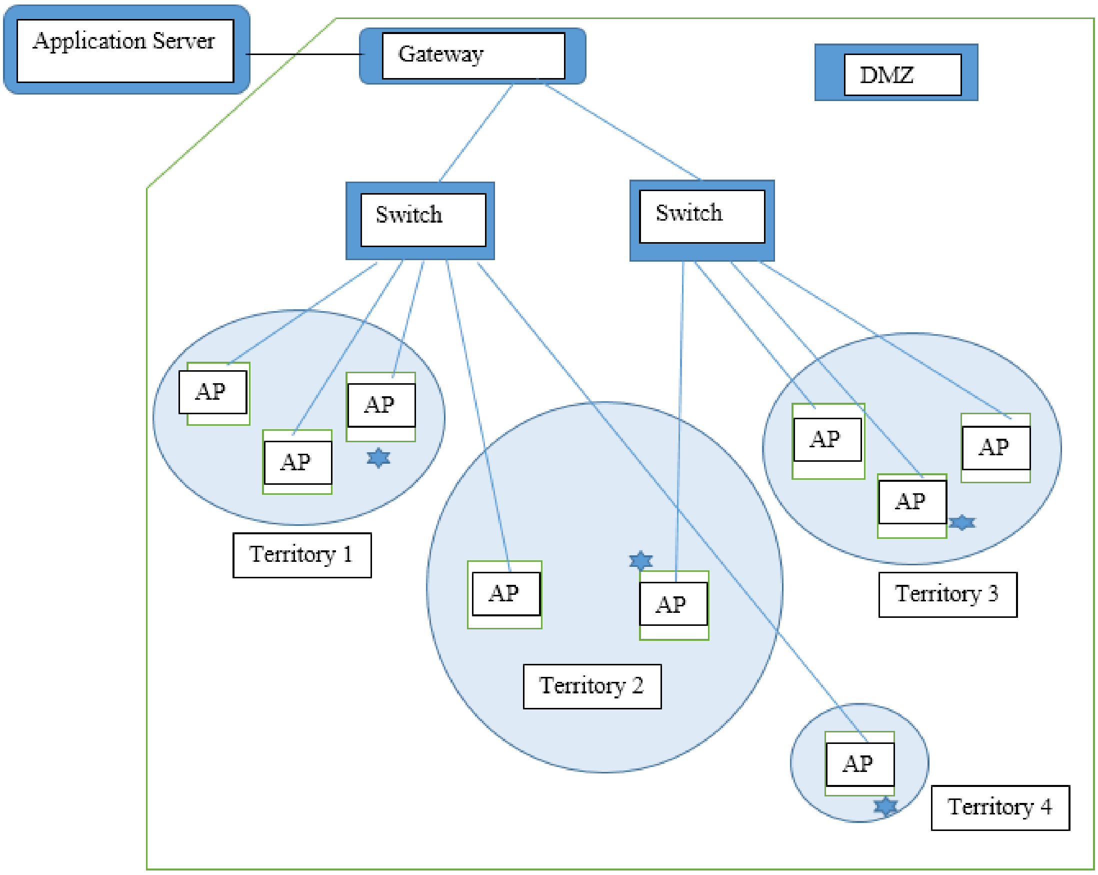


Figure 3.1: Architecture of the Deployment of System

3.1.3 Advantages

1. Mobile agent reduces network load, overcome network latency, encapsulate protocols, execute asynchronously and autonomously, adapt dynamically, naturally heterogeneous, robust and fault-tolerant.

2. In proposed monitoring system, mobile-agents are sent to continuously monitor nodes in a network, perform data filtering, reporting locally, and notify other system components of any momentous events over the network. The intelligent mobile agents will quickly sweep all possible RAPs, without generating loads of traffics on the network, hence saving resources. During the experimentation, it was observed that the proposed approach can robustly detect RAPs with minimal network overhead.

3.1.4 Results

The mobile agent based method is compared with existing method as shown in table 3.1. This implemented method can detect RAPs over wider area of 300 feet in less than one minute.

Table 3.1 Comparison of Results

Parameter	Existing System	Implemented System
Distance	150 ft.	In between 150 to 300 ft.
Network Latency	Marginal	Negligible
RAP Detection Time	1 Min	Less than 1 Min

3.2 WLAN Evil Twin AP Prevention Using Computational Approach

The locality of Evil Twin access points is amongst the most difficult security concerns for system administrator because it takes vital information from the network. Attackers take benefit of the hidden Evil Twin Access Points in network to get free internet access and to view useful information. This technique briefly describes the topological differences between the normal AP and Evil Twin AP scenario. In the normal AP scenario, a user communicates with the remote server (DNS/Web) through the normal AP. In the Evil Twin AP scenario, the victim client communicates with the remote server through the APs. Thus, comparing with the normal AP scenario, the Evil Twin AP scenario has one more wireless hop. This fact gives the intuition to detect Evil Twin attacks by differentiating one-hop and two-hop wireless channels from the user-side to the remote server.

3.2.1 Evil Twin Attack

An Evil Twin attack is very easy to install as shown in Figure 3.2. In public Wi-Fi area, like a coffee shop, airport, and restaurants, the attacker can easily set up Evil Twin access point which looks like an authorized access point. Evil access point set near victim then tries to attack the victim's wireless connection by using different methods and force the victim to change the connection. Evil AP use powerful wireless signals than the authorized AP. User's laptop automatically gets connected to AP with highest RSS. The attacker catches network packets between Evil AP and the authorized AP and get important information such as passwords, debit and credit card details [1].

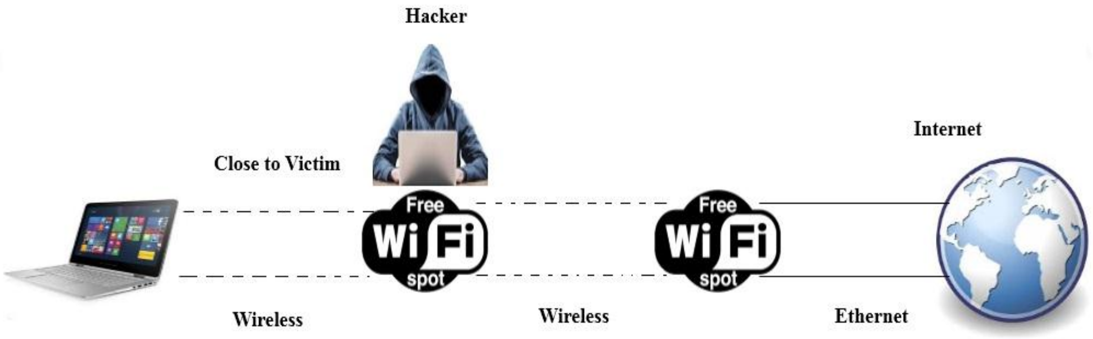


Figure 3.2 Evil Twin Attack

3.2.2 Evil Twin Access Point Detection

Proposed solution is installed on laptop as a detection/user client for communicating with a server. Further for an Evil Twin access point scenario, other wireless access points are deployed with similar Service Set Identifier as authorized AP. The Evil Twin access point (attacker) connects to the server through access point. In such scenario, the detection/user client transmits data to the server using a two-hop wireless channel. Evil Twin access point can also get connected through multi-hop wireless channels.

3.2.3 Network Setup

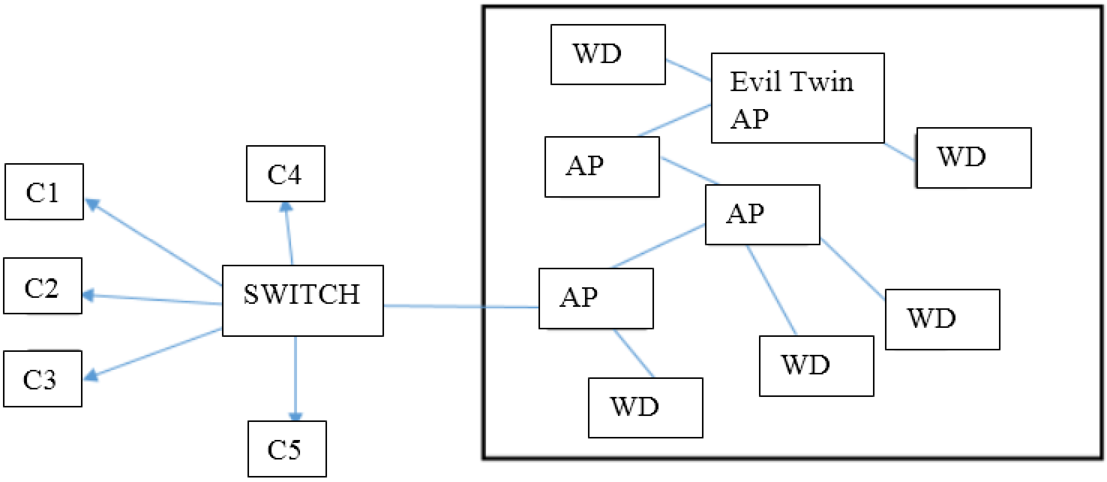
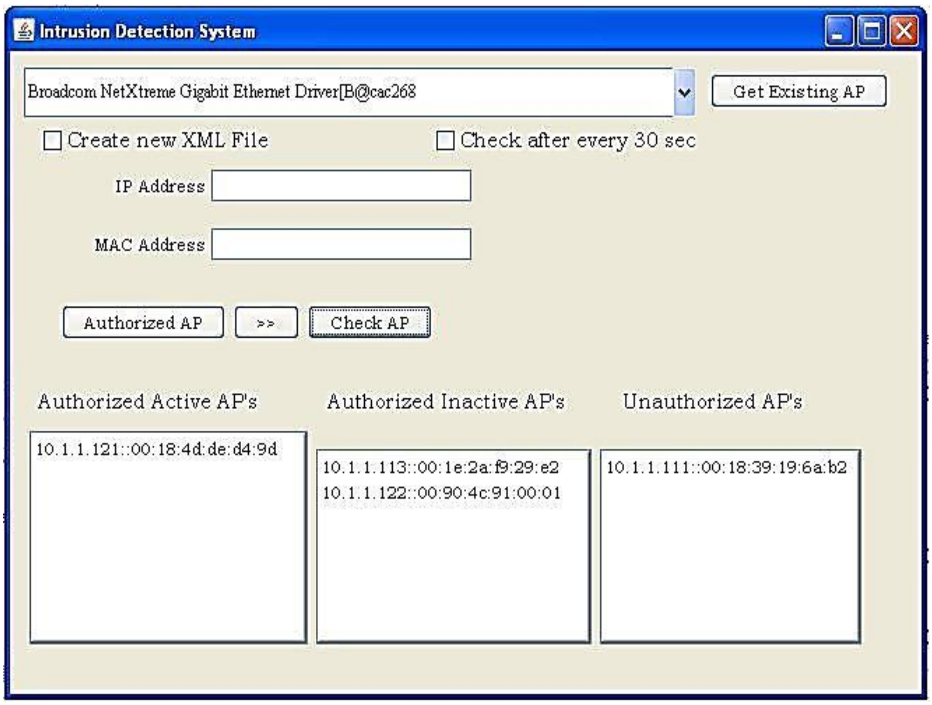


Figure 3.3 System Architecture

Figure 3.3 shows the system architecture where C1, C2, C3, C4, C5 are computers, AP- access point, WD- Wireless Devices. In this setup one access point is directly connected to the switch and other access points are connected with each other. Various wireless devices are connected to these access points. Desktop computers (C1, C2, C3, C4, C5) are connected to the switch. Evil Twin access point will try to connect to any authorized access point and present itself as the legal one. Wireless devices present in the network consider such Evil Twin access point as legal one and establish connection with it.

This application is tested with four APs with one AP as RAP and three APs as authorized APs. When AP button is selected the information like MAC address and IP address of the existing access points on the network is collected and it is compared with that of the authorized APs IP and MAC address information stored in data base. If the information does not match, then that access point is detected as RAP. Figure 3.4 shows the list of authorized access points will be displayed in authorized AP window, while unauthorized AP window displays the list of unauthorized access points.

3.2.4 Results



Broadcom NetXtreme Gigabit Ethernet Driver[B@cac268

☐ Create new XML File ☐ Check after every 30 sec

Authorized Active AP's

10.1.1.121::00:18:4d:de:d4:9d

Authorized Inactive AP's

10.1.1.113::00:1e:2a:f9:29:e2
10.1.1.122::00:90:4c:91:00:01

Unauthorized AP's

10.1.1.111::00:18:39:19:6a:b2

Figure 3.4 Output Snapshot

3.2.5 Advantages:

- Detects Evil Twin Attack for any type of network. (Wired or Wireless)
- Accurate detection of Evil Twin Access Point
- The solution is scalable.
- Consumes very less network bandwidth
- This technique can work on any type of network that is wired network, wireless network or heterogeneous network.

3.3 Detection of Fake AP in WLAN Using Received Signal Strength

The primary goal of this technique is to detect fake access point (FAP) in wireless environment by using received signal strength (RSS) value. A fake access point is a WAP which could be installed on a secured network of company without explicating the authorization from the management of local network. It is being created to allow an attacker to perform a Man in the Middle Attack [3].

3.3.1 System Architecture

FAP detection mechanism works in two modes as shown in figure 3.5. First mode is utilized for creating an authorized AP list known as learning mode. Second mode known as detection mode is utilized for detecting FAP in a network.

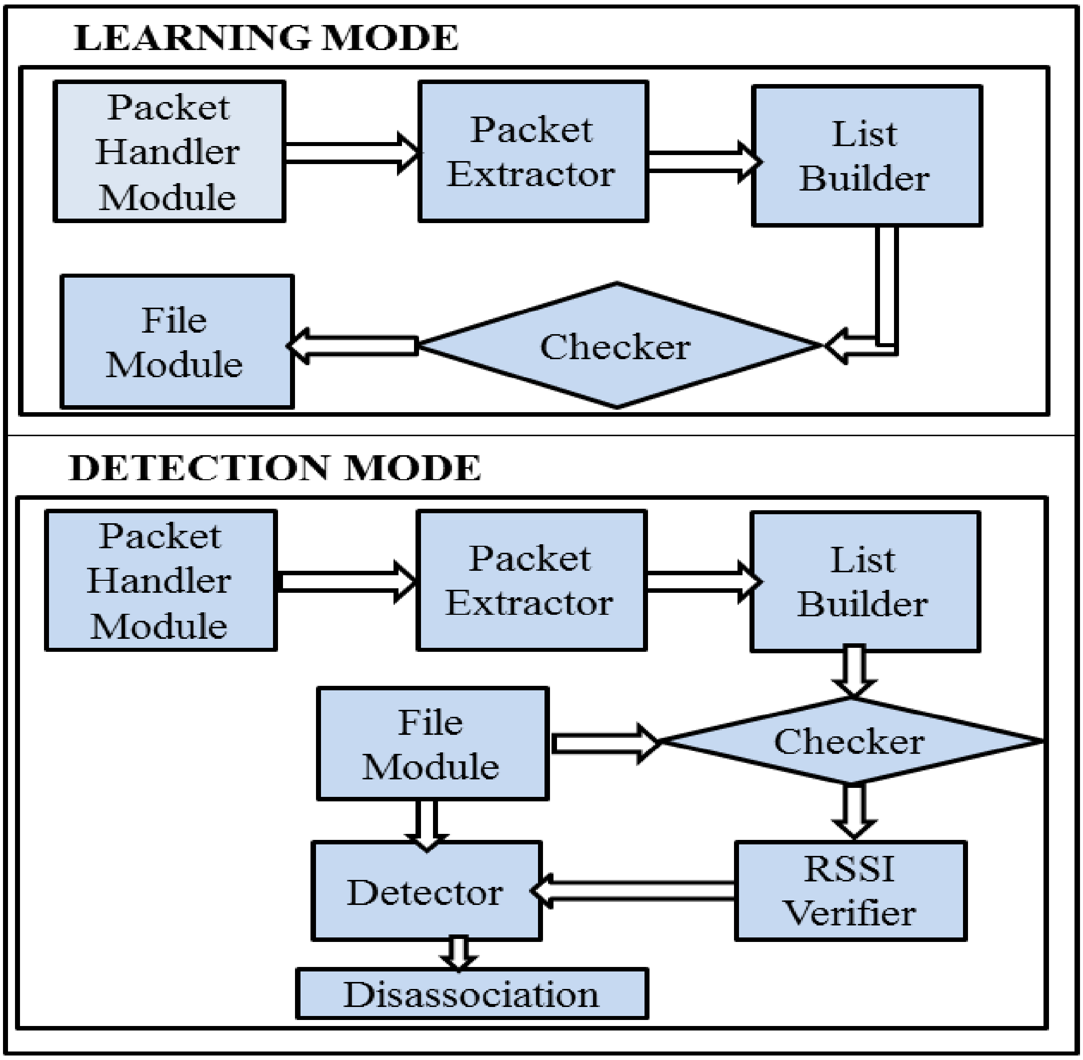


Figure 3.5 RAP Detection Using RSSI

3.3.1.1 Architecture for Learning Mode

Learning mode is utilized for creating white list called as authorized AP list. Network administrator uses this mode for maintaining list of all the authorized access points. White list contains information such as SSID, MAC address and RSSI values. An updated white list is used as an input for detection mode. Initially system is started in learning mode considering all available APs to be authorized access points for collecting their details.

3.3.1.2 Packet Handler Module

It is used to capture management and beacon frame in WLAN. Freeware tool Airmon-ng is used to capture and analyze the wireless packets.

3.3.1.3 Packet Extractor

It is utilized for extracting the information from captured frame, where the information includes MAC address, SSID and received signal strength of AP. It extracts the packet received from the packet handler module to identify the packet header field through which it can capture the information of SSID and MAC address.

3.3.1.4 List Builder

It is used to create a list of access points in network with detailed information. It creates a white list which is also called a Legitimate AP list. List builder uses the parameter like SSID, MAC address and RSSI.

3.3.1.5 Checker

Checker performs the very important task of verification of SSID and MAC address. In learning mode it is used to update the list builder information, which helps to avoid duplicate entries in white list.

3.3.1.6 File Module

It contains a file, which stores the records of access points in the white list.

3.3.2 Architecture for Detection Mode

3.3.2.1 Detection Mode

The system detection mode is enabled by default. In detection mode, first check for the SSID, if found by the system it looks for duplicated SSID or two access points that have similar SSID, and then it searches for MAC address of these two access points. If MAC address is similar, then it would consider it as an authorized access point even if it has duplicate entries. If it has a distinct MAC address then it checks its RSS indicator. If value of RSS indicator is similar to the whitelist or is smaller than or larger than the actual values and the contrast is +10 to -10 then it was considered as authorized access point else it generates a warning message. The administrator of network then takes an action against that specific access point by making use of policy of prevention. In detection mode packet handler, packet extractor, List Builder has same functionality as in module learning mode.

3.3.2.2 Checker

Checker performs the very important task of verification of SSID and MAC address. In detection mode it is used to verify the SSID, MAC address of all the APs for detecting FAP.

3.3.2.3 File Module

It contains the authorized access point list. It is used by checker and detector to identify FAP.

3.3.2.4 RSSI Verifier

It verifies the signal strength value of each AP. For example, if one AP has a signal strength value of -50 in white list. After execution of detection mode if the value of same access point is changed by ±10 than actual value, then it is considered as authorized access point. The value may not match exactly because of the effect of environmental conditions on signal strength. If the values are showing huge differences from original values, then it is considered as FAP.

3.3.2.5 Detector

It contains the information about FAP.

3.3.3 Prevention Policy

3.3.3.1 Prevention Mode

Prevention mode block the access points which are listed in black list. A black list consists of information about FAP. This black list contains SSID, MAC address and RSSI of blocked access points. FAP in a network can be blocked by using its SSID and MAC address.

3.3.3.2 Disassociation

In disassociation the FAPs are blocked. The system architecture is very useful for network administrator to reduce the workload.

3.3.3.3 White list

This list contains the information about all the authorized access points in the wireless network.

3.3.3.4 Black list

This list contains the information about all the FAPs in the wireless network. By using these two list network administrator easily identify authorized and unauthorized access point in the network.

3.3.4 Implementation

The method is implemented in Python. The applications used are Airmon-ng of aircrack suites for wireless traffic capturing. The Airmon-ng is helpful in capturing the enciphered traffic in wireless medium. Scapy library of python was used for the sake of packets handling and capturing. Initially management and beacon frames in a WLAN are captured. Packet Extractor is utilized for extracting the packets being captured and to read the details from various fields of packets.

In detection mode, the management and beacon frames of every access point in network are captured to get its SSID, MAC address and RSS Indicator from builder list. First of all it checks the SSID from the listing. If more than one access points have same SSID then it checks the MAC addresses of these two access points. If the same MAC address is found then it is considered as a duplicated entry of similar access point. But if the MAC address is distinct then checking of RSSI value is done. RSSI value is used for detecting FAP. The RSS signal variation is considered between 100 and 0. Where 0 says that the device was exactly at the place of detector and -100 says it is far away.

3.3.5 Experimental Results

This application is tested in a college network with seven authorized access point and one RAP. Tables 3.2 and 3.3 show the list of authorized APs in learning mode and unauthorized APs in detection mode, respectively.

3.3.5.1 Learning Mode

Table 3.2: Authorized AP List

Sr. No.	SSID	MAC Address	RSSI
1	Android AP	00:02:6f:5f:39:a3	-94
2	SST	20:10:7a:39:db:39	-78
3	BVCOEW	f8:1a:67:a1:06:cd	-93
4	Nano-con	bc:79:ad:52:81:ae	-40
5	IDEA-GPRS	00:7a:39:db:39:f8	-39
6	BVOCEP	52:81:5f:39:06:cd	-52
7	BVG	06:cd:ad:52:6f:5f	-49

3.3.5.2 Detection Mode

Table 3.3: Unauthorized AP List

Sr. No.	SSID	MAC Address	RSSI
1	**Android AP**	**00:02:6f:5f:39:a3**	**-94**
2	SST	20:10:7a:39:db:39	-78
3	BVCOEW	f8:1a:67:a1:06:cd	-93
4	Nano-con	bc:79:ad:52:81:ae	-40
5	Android AP	00:02:6f:5f:39:a3	-22
6	IDEA-GPRS	00:7a:39:db:39:f8	-39
7	BVOCEP	52:81:5f:39: 06:cd	-52
8	BVG	06:cd:ad:52:6f:5f	-49

3.3.6 Advantages:

- Method can be effortlessly deployed on any network.
- It detects RAP without addition of extra device for monitoring in a network.
- It does not require any alteration in the access point devices.
- Detection of RAPs is possible even though the traffic is enciphered.

3.4 Illegal Access Point Prevention in Wireless LAN Using Clock Skews

This technique helps the end users to detect the Fake AP on their network. For this purpose LSF (Least Square fitting method) algorithm is used. Jnetpcap tool was used to scan the wireless network using passive approach and gather the needed information from nearby wireless access points 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. This "timeval" parameter is used to calculate "clock skew" of each access point. Clock skew of access point is measured and stored to check the 'timeval' field in next scanning interval again to check whether the AP is fake or not. The threshold value is kept 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 which bigger than the threshold then it is fake AP.

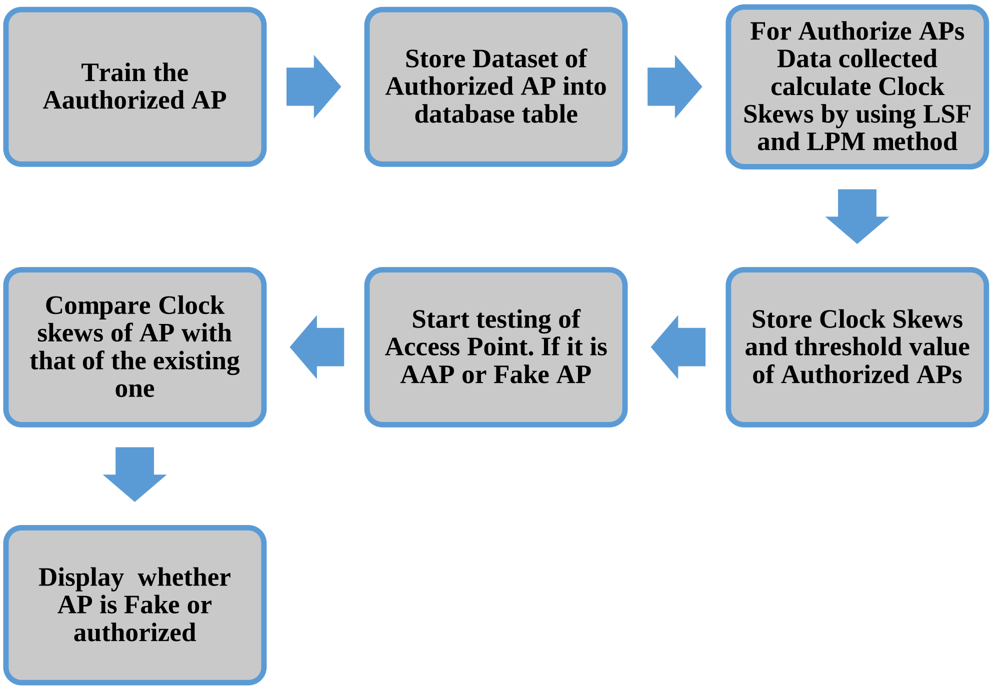

Train the Aauthorized AP
Store Dataset of Authorized AP into database table
For Authorize APs Data collected calculate Clock Skews by using LSF and LPM method
Store Clock Skews and threshold value of Authorized APs
Start testing of Access Point. If it is AAP or Fake AP
Compare Clock skews of AP with that of the existing one
Display whether AP is Fake or authorized

Figure 3.6 System Execution Sequence

3.4.1 System Execution Sequence

As shown in figure 3.6 there are four main steps : First step is for training the authorized AP, next is for calculating clock skews by using LSF and Linear Programming Method (LPM) for authorized APs collected data, followed by calculating and comparing clock skew values of AP under test with already stored authorized APs clock skews. Last step displays the result and graph to the user.

Step 1: Train the authorize AP:

This step is needed to train the authorized AP. It is responsible to connect an authorized AP and received beacon frames.

Step 2: Authorized APs data collected to calculate clock skew values:

This step is responsible for calculating clock skew of authorized access point. The clock skew can be calculated by using number of beacon frames received from authorized AP in previous step. The clock skew value can be estimated by using LPM and LSF method. This data has to be stored into database.

Step 3: Calculating and comparing clock skew values of AP:

This step is responsible for collecting test data of AP which has to be tested. Again the beacon frames are received and clock skew value is calculated. This value is compared with a value in database which is already stored.

Step 4: Display Result

This step will show result in the form of message and graph.

3.4.2 Implementation

Two modules were implemented to prevent RAP in wireless LAN using clock skews:

Module 1: Training authorized AP

Module 2: Calculating the clock skews and threshold value of AP

3.4.2.1 Results

Table 3.4: Estimation of Clock Skew Values of Access Point

Number of Packets Examined	Estimation of Clock Skews	
	Skew (using LSF)	Skew (using LPM)
100	19.74 ppm	30.29 ppm
200	34.71 ppm	11.03 ppm
300	51.86 ppm	24.10 ppm
400	26.86 ppm	29.17 ppm

Table 3.4 shows the estimation of clock skew values of access point using LSF and LPM algorithms for different number of packets examined.

3.4.3 Advantages:

- RAP is detected using clock skew. So RAP detection accuracy is high.

3.5 Providing Data Security in WLAN by Detecting Unauthorized Access Points and Attacks

In this technique two different modules have been designed. First module is used for detection of unauthorized access points. Second module is used for detection of network attacks performed by authorized as well as unauthorized access points. It also drops all the packets which come from unauthorized access point, so that it does not achieve the purpose for which it is connected.

3.5.1 MODULE 1: System Architecture of Unauthorized Access Point Detection in WLAN

In this method three types of access points are considered:

- Authorized
- Unauthorized
- External

Authorized APs are configured by network administrator. External APs belongs to external network, so such APs should be discarded. External APs spoof the SSID or MAC address of authorized AP to divert network traffic through access point. Using different levels of filtering such access points can be detected. The first filter is to check SSID or MAC address of AP. If SSID is different, then it might be the AP of external network. If SSID or MAC is of same network then second level of filtering using IP and MAC is used. IP and MAC values are compared with stored database, if match is found then access point is authorized else unauthorized. Third level of filtering is applied for MAC spoofing.

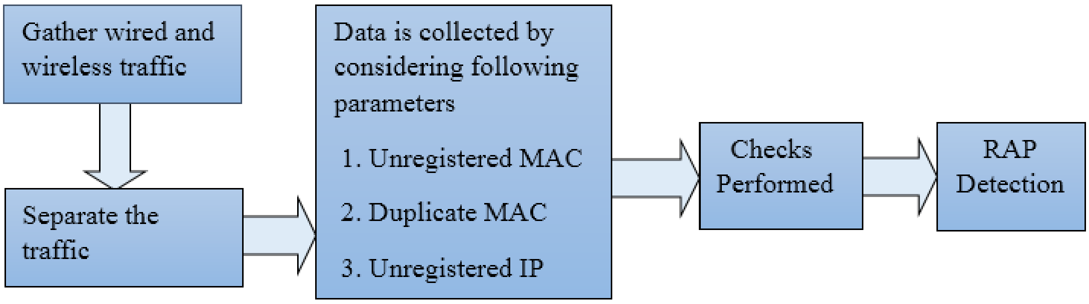


Figure 3.7: System Architecture of Unauthorized Access Point Detection in WLAN

As shown in figure 3.7 first packets were captured and then the traffic is separated to consider wireless packets only. Packets are collected by considering unregistered MAC, duplicate MAC and unregistered IP. Then checks are performed with stored database and RAP is detected.

3.5.2 MODULE 2: System Architecture of Network Attack Detection

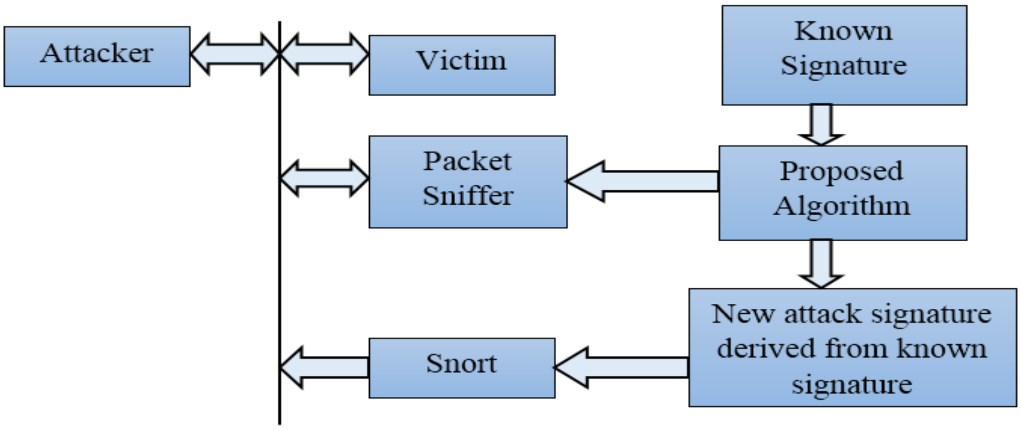


Figure 3.8: System Architecture of Network Attacks Detection

From the attack signatures, it is found that some attack signatures are similar to other attack signatures generated previously. This is due to the new attack which gets generated is a derivative of the previous known attack. For example, worms. All worms are similar because the main task of any worm is to consume network resources by propagating itself in the network and eventually force the system to halt.

So some part of the known signature is used to find out the new attack signatures. To generate candidate item sets and scan the database traditional Apriori algorithm could be used, but it takes too much time. Therefore, an algorithm to identify intrusions by making use of old signatures, which will save a lot of processing time, was suggested.

As shown in Figure 3.8 attacker gets an attacking tool to attack victim. The algorithm in this technique uses data that comes from packet sniffer and known signature. Algorithm output is the new attack signatures derived from known signatures. Signature accuracy is checked using snort.

3.5.3 Advantages:

- This technique can detect RAPs as well as identify the network attacks.
- System detects RAPs and also drops all the packets send by RAP, thus nullifying the effect of the attack.
- This technique does not require any extra sensors and hardware.
- Displays continuous warning about the prevented attacks.
- Network administrator can view existing signatures.
- Provides a log file of all the prevented attacks.

3.6 Illegal Access Point Detection for Wi-Fi Network by Using Hybrid Approach

In this technique, a practical hybrid framework is developed targeting pre-empting attacks that can create RAPs, and detecting the presence of such devices. It is the first framework that correlates alerts containing all data from both wired scans and wireless surveillance. An attractive feature of the proposed framework is that it requires neither specialized hardware nor modification to existing security standards. Further, it can be connected to or implemented on APs as small plugins. It also makes use of freely available mature software in order to provide a cost-effective security solution. It can protect networks from RAPs even when assuming that adversaries have the ability to use customized equipment that violates the IEEE 802.11 standard.

In this technique two different modules are developed. First module is used for detection of unauthorized access points for centralized system. Second module is used for detection of unauthorized access points for distributed system.

3.6.1 System Architecture of Illegal Access Point Detection in Wi-Fi Network

3.6.1.1 Illegal Access Point Detection (IAPD)

In most enterprises wireless implementations contain the wireless security measure such as IEEE 802.11i or WPA (Wireless Protected Access) or WPA-2. IEEE 802.11i provides the authentication and encryption mechanisms to defend users from unauthorized access and data. However, such security measures cannot protect the system from the unauthorized installation of the access point by their own staffs. Network defenses through the RAP pose serious threat to the organization. Network can be safe after detecting and eliminating the RAP for Wi-Fi network by using hybrid approach.

3.6.1.2 Understanding Hybrid Networks

Any computer network that contains two or more different communications standards is hybrid network. The hybrid network uses both Ethernet (802.3) and Wi-Fi (802.11 a/b/g/n) standards. A hybrid network depends on hybrid routers, hubs and switches to connect both wired and wireless computers.

- To monitor network activities hybrid framework is designed, forestall events that could lead to the generation of RAPs, discover existing RAPs, and block unauthorized network access through RAPs.
- Two main components that constitute its architecture are
  1. The distributed monitoring module.
  2. The centralized detection module.

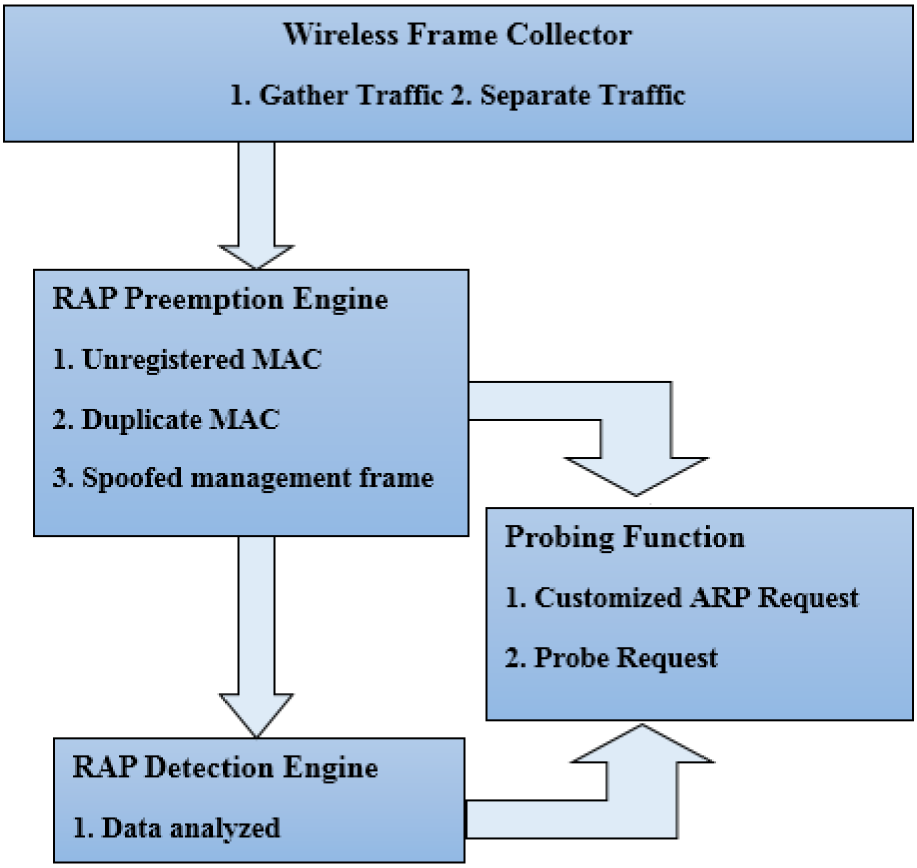


Figure 3.9 Distributed Monitoring Module

3.6.1.3 The Distributed Monitoring Module

This module consists of a wireless frame collector, a RAP pre-emption engine, and a RAP detection engine. As illustrated in Figure 3.9 the frame collector gathers wireless traffic. Data collected is then passed to the pre-emption engine, where different checks are performed in order to avoid various attacks. Then detection engine analyzed data. Probing functions shared by the pre-emption and detection engines, so that attackers can be lured into revealing their presence.

1. Wireless Frame Collector: A frame collector is used for real-time WLAN monitoring to quickly identify rogue wireless devices. Frame collector separates wired and wireless traffic. So no need of complicated modules that attempt to isolate the wired and wireless traffic by examining traffic signatures.
2. RAP Pre-emption Engine: Network attacks cannot be avoided, but it is possible to prevent attacks before occurrence.
   a) Eavesdropper Probing: Probing functionality is employed to help prevent class four rogues from network.
   b) Intruder Discovery: Following action is carried out on the data obtained from the wireless frame collector for integrity checks.
      - Unregistered MAC addresses
      - Duplicate MAC addresses
      - The presence of management frames
3. RAP Detection Engine: There are two primary reasons for the RAP detection engine. First, defending against class 1 to class 3 RAPs is an inherently reactive process. Second, by identifying traffic from an unauthorized user class 4 RAPs are detected.

Figure 3.10 shows the overall step-by step execution of distributed monitoring module in which first it will diffrentate the authorised and unauthorized AP. By observing the OS fingerprints it cheks the number of times the attack is to be done. After doing this the system will keep the track of the MAC address which will cheks for unregistered MAC and duplicate MAC.

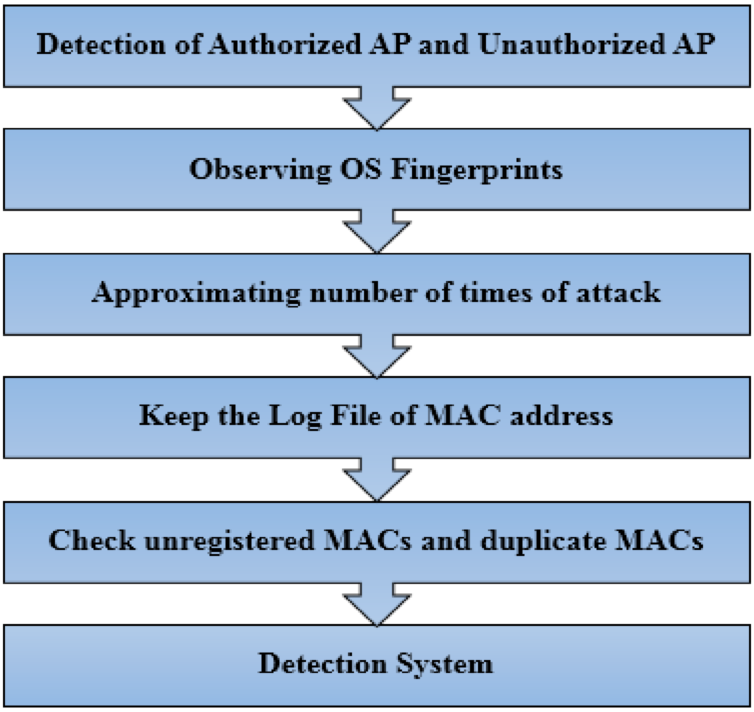

Detection of Authorized AP and Unauthorized AP
Observing OS Fingerprints
Approximating number of times of attack
Keep the Log File of MAC address
Check unregistered MACs and duplicate MACs
Detection System

Figure 3.10: Steps in Distributed Monitoring Module

3.6.1.4 Centralized Detection Module

The wireless distributed monitoring module is effective for spotting rogues, but those not within the coverage range may remain undetected. The ideal method of detecting such RAPs is to use a central console attached to the wired side of the network. Benefit of central point detection is that it alleviates the need to walk through the premises in case of incomplete coverage.

3.6.1.5 Advantages of IAPD

1. Extra features can be easily added in future due to its open architecture.
2. Framework is capable of detecting rogue devices and blocking potential attacks.
3. It correlates alerts containing all data from both wired scans and wireless surveillance.
4. It requires neither specialized hardware nor modification to existing security standards.

3.7 Unapproved Access Point Elimination in WLAN using Multiple Agents and Skew Intervals

3.7.1 Scenarios

Unapproved APs can operate in two scenarios.

1. Authorized AP and Unapproved AP (UAP) are both active in the network as shown in figure 3.11. A client can receive beacons from both the APs. The attacker can keep the signal strength of unapproved AP above that of authorized AP so that user will be forced to connect with the unapproved AP.

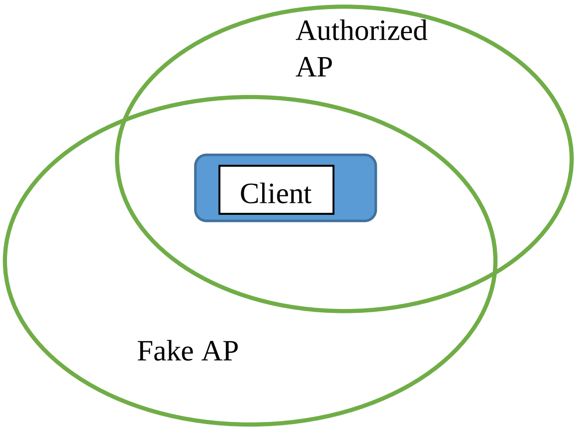


Figure 3.11: Threat Scenario 1

2. Only unapproved AP is active and authorized AP cannot be reached by the client as shown in figure 3.12. This can happen in some situations like failure of authorized AP due to internal reasons or due to attack by the adversary. The attacker can also follow the client beyond the field of influence of authorized AP.

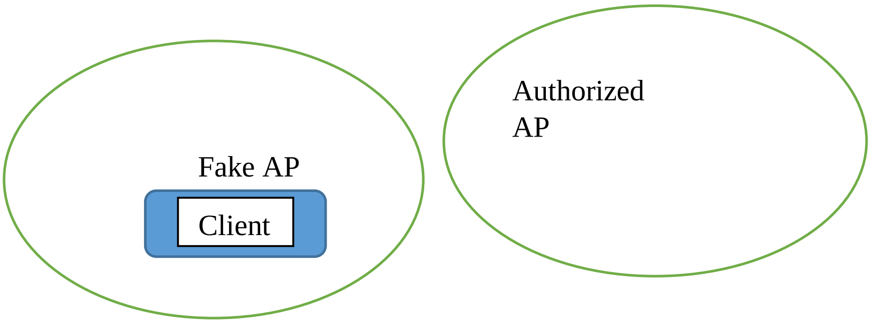


Figure 3.12: Threat Scenario 2

For calculation of skew interval, it is necessary to gather time measured by two different devices. Use of two types of timestamps had been done in this technique:

Source Timestamp – Beacon frame is sent by an access point, the device driver of the AP record the time of sending in the timestamp field of beacon header. This is called as source timestamp.

TSF Timestamp – Whenever a client receives a frame, the device driver on the client side records time of arrival as indicated by the client's skew into the timestamp field of Radio Tap Header. It is called as Time Synchronization Function (TSF) timestamps. These timestamps help in determining the exact skew interval between the WIDS node and access point.

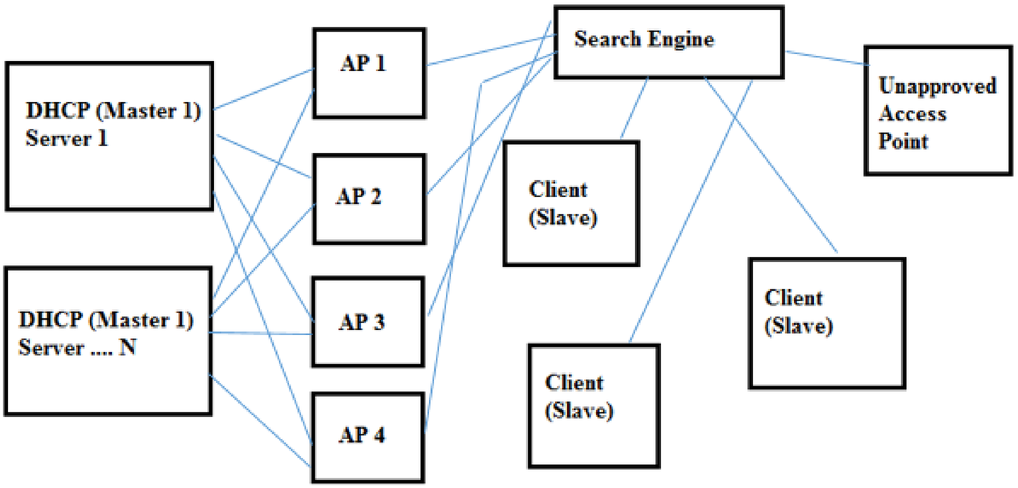


Figure 3.13: RAP detection using multiple agents and skew intervals

Here the concept of multiple servers as shown in figure 3.13 is used so that if one server crashes another server can be used to interact with the clients.

3.7.2 Implementation

This system automatically detect and eliminate UAPs by applying the mobile multi-agents to the network. Two different levels of mobile agents- Master and Slave Mobile Agents are being used.

Initially a master agent is generated on the DHCP-M server, which is responsible for regulating all the authorization processes of the wireless network. This master agent generates slave agents depending upon the number of active access points connected to the server at that moment of time. These slave agents are then dispatched on the connected APs respectively. Now these slave agents are cloned on every access points and are being dispatched to every client system connected to the APs. When the cloned slave agent detects any new access point at the client's system, it automatically builds and sends information packet INFO such as SSID, MAC-Address, Vendors Name, Channel Used of the unauthorized AP to clone agent of the connected AP. The slave agent at AP dispatches this information to its master agent on the server. Master agent calculates the estimated skew interval and also calculate new skew interval from first seen and last seen information and checks for these two skew intervals. If both are same, then the access points will be authorized. If the information is matched and the AP is found authorized then a new slave agent is generated and sent to that AP. If it is detected as a client MAC address, a disassociation frame is sent to all APs to inform them not to connect with it. If the details does not match with either of it then the MAC address of the AP is fetched from the INFO, the port at which the AP is connected is searched and then that AP is blocked for any LAN traffic.

Detection of Unapproved AP

Threshold and skew interval values are written to the file. The process is described below.

- Capture number of packets from each source to determine accurate skew interval.
- Based on threshold value, separate the packets into various data sets.
- Apply Least Square Fitting (LSF) on each of the datasets and calculate its estimated skew interval.
- If the beacons are having same MAC Address, SSID and BSSID but lying in different ranges of skew interval, then unapproved AP is present in the network.

3.7.3 Results

Comparison between existing system and proposed system for average detection time of access point, cost required and hardware required is shown in figure 3.14.

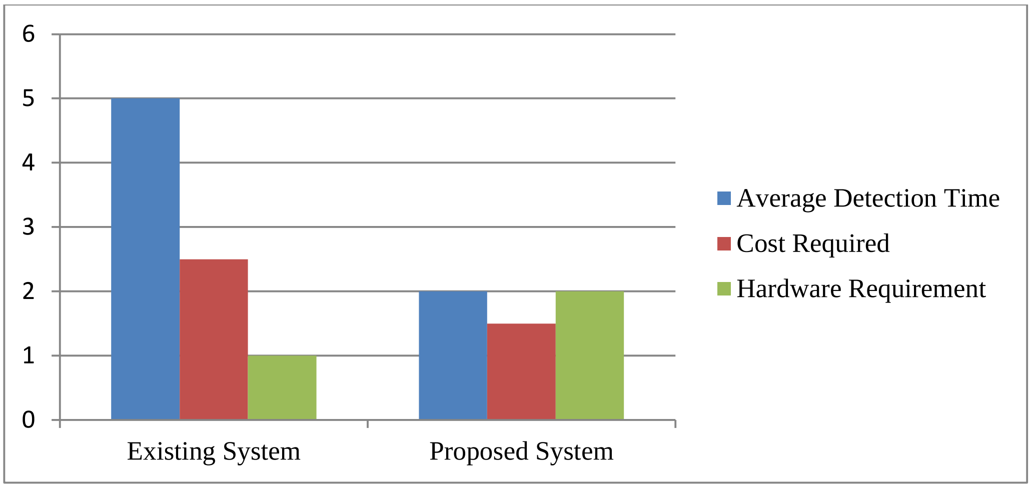


Figure 3.14: Comparison of accuracy in existing and proposed system

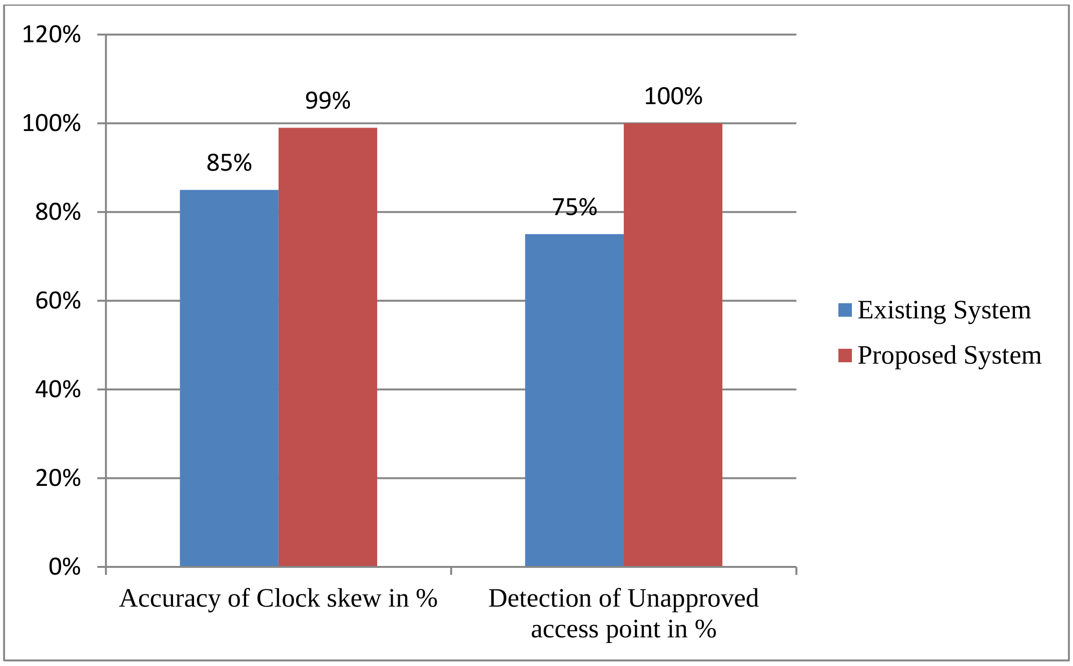


Figure 3.15: Comparison of clock skew in existing and proposed system

Comparison of clock skew in existing and proposed system is as shown in figure 3.15.

3.8 Summary of Contributions

As explained in sections above, seven different techniques were implemented for RAP detection. The experimental results were analyzed to understand the advantages and limitations of these techniques. These limitations observed during experimentation served as motivation to develop a more robust solution for RAP detection.

1. In mobile agent based RAP detection technique, all nodes in a network may not allow execution of mobile agent code on them. RAP may not allow installation of mobile agent code on it, so RAP will remain undetected.
2. The techniques used to detect Evil Twin attack has a constraint that it requires all the nodes to be in the same subnet. Also the time required to detect RAP is more.
3. While detecting the fake AP in WLAN using RSS and detecting illegal access point using clock skew, it was observed that change in environmental factors like, temperature, humidity etc., can also change the RSS as well as clock skew values because of which accuracy of RAP detection gets reduced.
4. The important drawback of the technique based on anomaly system is that the system must be trained to create the user profile. Maintaining the profile is a time consuming task. Also the solution has not been tested for real time attacks.
5. All these techniques consider only two or three parameters for RAP detection. So possibility of number of false positive cases is more.
6. Time required to detect RAP is more.
7. Clock skew value may change due to different factors.

Due to these limitations of implemented methods, the vulnerabilities stated above are observed in the implemented methods, using which intruders perform various attacks on WLAN. From these vulnerabilities, it was deduced that there is a need for considering some additional parameters. This acted as a motivation to design a system that considers multiple parameters for RAP detection.

The system design of Multiparameter RAP detection is presented in next chapter.

CHAPTER-4

DESIGN OF THE MULTIPARAMETER RAP DETECTION METHOD

4.1 Factors Affecting RAP Detection Techniques

The different factors which affect the RAP detection techniques are:

Received Signal Strength (RSS) Level- For detection of RAP different RSS levels of access point are used. So variations in RSS levels also causes variation in results.

Wireless Traffic- Some methods use wireless traffic between client and access point for detection of RAP. In wireless environment, sometimes the network traffic provides inaccurate results. But because of inaccurate results it creates a suitable environment for RAP to perform attacks.

Workload of Access Point- The effectiveness of detection of RAP is affected by workload of the access point.

Training Data- It is used to compare the obtained results for detection of RAP. Wrong training data can create a problem for the detection technique used.

When a user wants to connect to a wireless network, it uses a SSID to connect to the access point. The attacker creates an SSID which is same as a legitimate AP. It is quite difficult for users to identify the legitimate access point. SSID can be hidden by using network cloaking technique so that attacker does not know the SSID. There are a number of ways to get SSID. For example, when the SSID is sent through a frame it is in unencrypted format, making it easy for attacker to read it by capturing the frame. The attacker also uses sniffing programs, which is used to spoof a MAC address, logical address and SSID of an access point. Using such sniffing programs attacker can easily get the data of authorized access point which is used for authentication and create a RAP in the same network.

Every organization designs a network in such a way that it separates wired and wireless network and applies different security measures on each network. Despite this an attacker can easily break the security using sniffing program.

The wireless network solution is expensive and can be easily targeted by sniffing programs. Both these approaches work well in specific environment but do not have any assurance that they can provide security to latest mobile devices in public Wi-Fi.

4.2 Access Point Detection Parameters

4.2.1. SSID: It is a short form used for Service Set Identifier. SSID consist of 32 characters. There can be multiple access points with the same SSID in a single network. Using SSID all nodes in a network communicate and interact with one another.

4.2.2. MAC Address: It is a short form used for Media Access Control. MAC address is a unique identifier assigned to all network interfaces and is used for communication between physical network segments.

4.2.3. RSS: It is called Received Signal Strength. The superiority of communication between the sensor unit and the access point is indicated by the RSS value and is expressed in decibels (dB). The RSS values are always negative because of low power levels and attenuation of free air. Table 4.1 shows RSS value ranges for different signals.

Table 4.1 RSSI Value Range

RSS Value Range	Signal Quality
Greater than or equal to - 40 dB	Exceptional
-40 dB to -55 dB	Very good
-55 dB to -70 dB	Good
-70 dB to -80 dB	Marginal
-80 dB and beyond	Intermittent to no operation

RSS values can vary from 0 to -100. The value near 0 indicates robust signal whereas the value approaching -100 shows weaker signal.

4.2.4. Channel and Frequency:

Wireless channels are used to transfer information signals from one network to another network. Channels can transmit the information signals from senders to receivers. The transmission capacity of the channel is expressed in terms of its bandwidth (Hz) or data rate (bits per second).

As shown in table 4.2, total 13 unlicensed channels exist in the wireless network. Every channel has a unique frequency range from 2412 MHz to 2484 MHz with a difference of 5 MHz each.

Table 4.2 Channels and Frequency

Channel	Frequency	Frequency Spread
1.	2412 MHz	2399.5 MHz - 2424.5 MHz
2.	2417 MHz	2404.5 MHz - 2429.5 MHz
3.	2422 MHz	2409.5 MHz - 2434.5 MHz
4.	2427 MHz	2414.5 MHz - 2439.5 MHz
5.	2432 MHz	2419.5 MHz - 2444.5 MHz
6.	2437 MHz	2424.5 MHz - 2449.5 MHz
7.	2442 MHz	2429.5 MHz - 2454.5 MHz
8.	2447 MHz	2434.5 MHz - 2459.5 MHz
9.	2452 MHz	2439.5 MHz - 2464.5 MHz
10.	2457 MHz	2444.5 MHz - 2469.5 MHz
11.	2462 MHz	2449.5 MHz - 2474.5 MHz
12.	2467 MHz	2454.5 MHz - 2479.5 MHz
13.	2472 MHz	2459.5 MHz - 2484.5 MHz

4.2.5. Authentication Type: User in any network wants security of its data being transferred from source to destination. The transmission protocols and policies for secured communication are known as authentication.

4.2.6. Timestamp: It indicates time of the event recorded by computer. It contains the information which indicates the exact occurrence of the event. This information is useful for calculating the clock skew value.

4.2.7. Sequence Count: It is a number in the beacon frame which is incremented by 16 with every beacon frame transmission.

4.2.8. Clock Skew: The difference between two successive timestamps is called as clock skew. Clock skew value remains consistent for same AP.

4.3 Wireless Architecture

In wireless architecture variety of network and computing devices are used. As wireless LANs use high frequency radio signals the area covered by them is usually very limited. This limited area is called as Basic Service Set (BSS). Every BSS area in wireless LANs has an identifier. This identifier is known as Service Set Identifier (SSID). Inside every BSS there are several computing and networking devices which have Wi-Fi network interface cards (Wi-Fi NICs). These cards are of two types. First type is used by wireless access points and the other is used by wireless devices, which have to connect to wireless access points. Description of various terms used in wireless architecture is as given below.

Basic Service Set (BSS): Basic Service Set is a set that contains all the computing and networking devices along with all wireless access points. It is the network that contains single wireless access point.

Access Point: It is the device that works at data link layer and has unique MAC ID. This device runs various data link layer protocols for IEEE 802.11. By using this device, wireless end devices communicate with each other as this device acts as wireless gateway.

Clients: Clients here are the wireless end devices that run IEEE 802.11 protocols. They usually get connected to wireless access point for connectivity.

Service Set Identifier (SSID): BSS are identified by their SSID. SSID has size of 32 bytes. It is the name associated with any wireless IEEE 802.11 LAN. Each device in the network has a unique SSID.

Channel: Various frequencies in between 2 GHz to 5 GHz are used for deploying wireless LANs. These frequencies use radio signals as wireless medium for data communication and have several channels inside. In many countries different number of channels are used. Usually 2.4 GHz frequency range is divided into 14 channels, separated by 5 MHz. If the channels are not properly used, they may overlap each other and create interference. Hence while deploying wireless LAN care should be taken when deciding wireless channels.

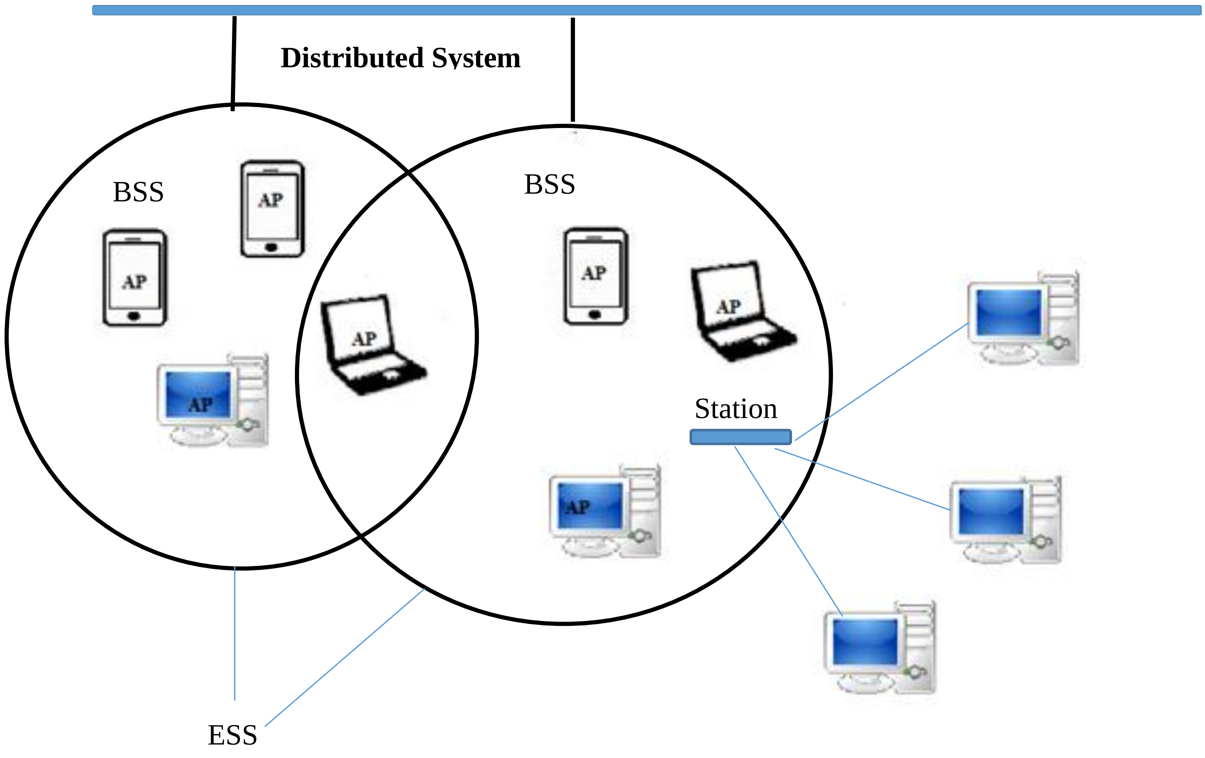


Figure 4.1: Architecture of Wireless LAN

Figure 4.1 shows a typical wireless LAN architecture. It consists of two wireless LANs with two BSS. These two networks collectively have one extended service set (ESS). This network has several wireless clients who use radio frequencies and various channels to get connected to wireless access points. A wireless network with several access points is called ESS.

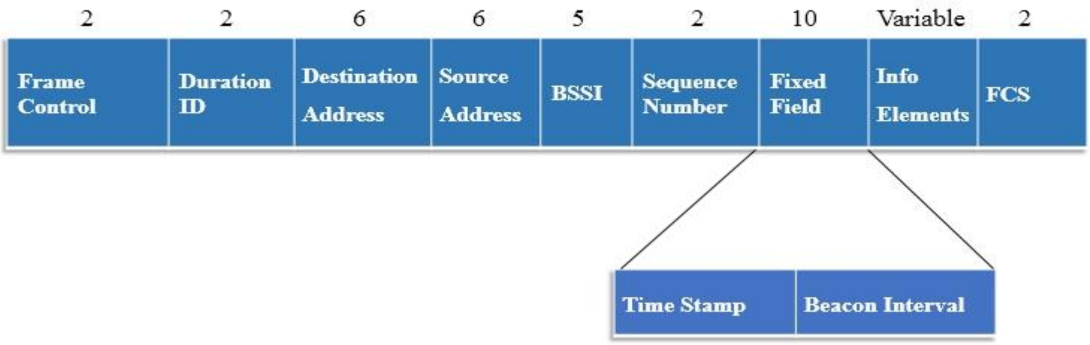
Beacon Frame: In IEEE 802.11 WLAN, beacon frame is management frame. It contains all network details. Beacon frames are transmitted frequently by access point to announce presence of wireless LAN. Beacon frame is approximately fifty bytes long containing cyclic redundancy check (CRC) field and common frame header. Source and destination MAC addresses are included in header. CRC field detects error.

The body of beacon frame carries following information:

- **Beacon Interval -** It is the time between two beacon transmissions. Station should know when to wake up to receive the beacon before a station enters power saving mode.

- **Timestamp -** Timestamp value from beacon frame is used by station to update its clock. This method enables synchronization among all devices that are connected with the same access point.
- **Supported Rates -** Each beacon frame carries information that defines the rates that the wireless LAN supports. Stations use performance metrics to decide which access point to associate.
- **Parameter Sets -** The information about the signaling methods is stored in beacon frame. Hopping pattern and dwell time of frequency hopping network is indicated in beacon.
- **Capability Information-** It is the indication of requirement of the stations that belong to beacon representation of the wireless LAN.
- **Traffic Indication Map (TIM) -** Stations using power saving mode are identified from TIM sent by access point periodically, to identify which stations are having data frames to wait for access point's buffer.

Figure 4.2 shows a beacon frame structure of wireless LAN.

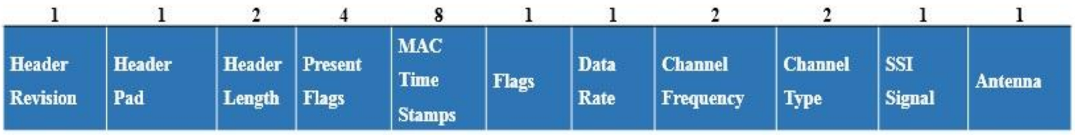


2	2	6	6	5	2	10	Variable	2
Frame Control	Duration ID	Destination Address	Source Address	BSSI	Sequence Number	Fixed Field	Info Elements	FCS

Figure 4.2: Frame Structure of Beacon Frame

Radio Tap Headers

Figure 4.3 shows structure of radio tap of header. Length of this header is 32 bytes. It contains information like data rate, SSI signal and channel frequency, MAC address, time stamps, channel type, header pad and various flags. These values can be used for variety of operations, from management to administration.



1	1	2	4	8	1	1	2	2	1	1
Header Revision	Header Pad	Header Length	Present Flags	MAC Time Stamps	Flags	Data Rate	Channel Frequency	Channel Type	SSI Signal	Antenna

Figure 4.3: Structure of Radio Tap of Header

4.4 Architecture

Figure 4.4 describes the architecture of implemented system.

4.4.1 Learning Mode: Learning mode creates a white-list called authorized AP list. It contains details of authorized access points. This includes MAC address, SSID, RSS, channel and frequency, encryption. An updated white-list is applied as an input to detection mode. Initially the system starts in learning mode considering all available APs are authorized, and collects the following information about them.

- **Beacon Frame Extractor**: It is used to extract the information from captured beacon frame using scapy library. The information like MAC address, SSID, frequency, RSS Value, and channel etc. are extracted and made available for further operations.
- **SSID Reader:** It is used to extract and read the SSID of the considered AP from captured beacon frame.
- **MAC Reader:** It is used to extract and read the MAC address of the considered AP from captured beacon frame.
- **Frequency Reader:** It is used to extract and read the frequency value from captured beacon frame.
- **Channel Reader:** It is used to extract and read the channel number used by the AP from the captured beacon frame.
- **Encryption Reader:** It is used to extract and read the encryption used by the AP from the captured beacon frame.
- **RSS Reader:** It is used to extract and read the signal strength value from captured beacon frame.
- **Clock Skew Reader:** It is used to extract and read the timestamp value from captured beacon frame. It also generates the clock skew value by calculating the difference between two timestamps.
- **Sequence Count Reader:** It is used to extract and read the sequence count from the captured beacon frame.
- **Policy Generator:** It is used to generate the white-list of the authorized APs. This list is used as the input to detection mode.

4.4.2 Detection Mode:

Detection mode is the default mode of the system. In this mode, first the SSIDs of all detected APs are checked. If two APs have the same SSID, then MAC addresses of these two APs are checked. It also considers other parameters like MAC address, frequency, RSS, clock skew and sequence count. Even if a single value is detected to be mismatched, then that AP is considered as rouge. This mode of operation is explained as below:

- **Beacon Frame Extractor:** It extracts the information from captured beacon frame using scapy library. The parameters like MAC address, SSID, Frequency, RSS Value, and Channel are extracted and made available for further operations.
- **SSID Checker:** SSID of the detected APs are compared to check if there are two or more entries with the same SSID.
- **MAC Checker:** If two or more APs have the same SSID, then the MAC address is compared with the entries in the white-list. If a match is found with the entry in the white-list then it is an authorized AP, else it is RAP.
- **Frequency Checker:** If two or more APs have the same MAC address, then the frequency of the duplicate APs are compared with the corresponding entry in the white-list. The one which matches with the entry in the white-list is the authorized AP, else it is RAP.
- **Channel Checker:** If two or more APs have the same frequency, then the channel number of the duplicate APs is compared with the corresponding entry in the whitelist. The one which matches with the entry in the whitelist is the authorized AP, else it is RAP.
- **Encryption Checker:** If two or more APs have the same channel, then the encryption used by the duplicate APs are compared with the corresponding entry in the whitelist. The one which matches with the entry in the white-list is the authorized AP, else it is RAP.
- **RSS Checker:** If two or more APs have the same channel number, then the RSS values of the duplicate APs are compared with the corresponding entry in the white-list. The one which matches with the entry in the white-list is the authorized AP, else it is RAP.
- **Clock Skew Checker:** If two or more APs have the same RSS value, then the clock skew values of the duplicate APs are compared with the corresponding entry in the

whitelist. The one which matches with the entry in the white-list is the authorized AP, else it is RAP.

- **Sequence Count Checker:** If two or more APs have the same clock skew value, then the sequence count of the duplicate APs is compared with the corresponding entry in the white-list. The one which matches with the entry in the white-list is the authorized AP, else it is RAP.

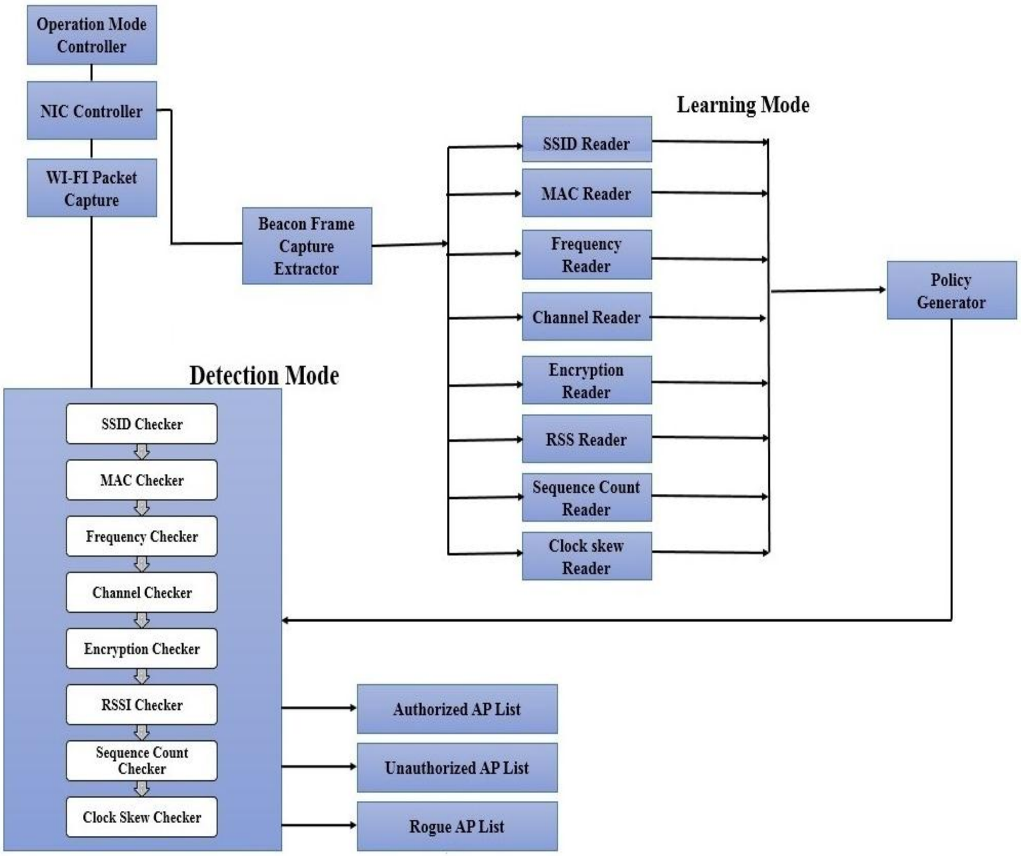


Figure 4.4: System Architecture of Implemented Approach

4.5 Flowchart

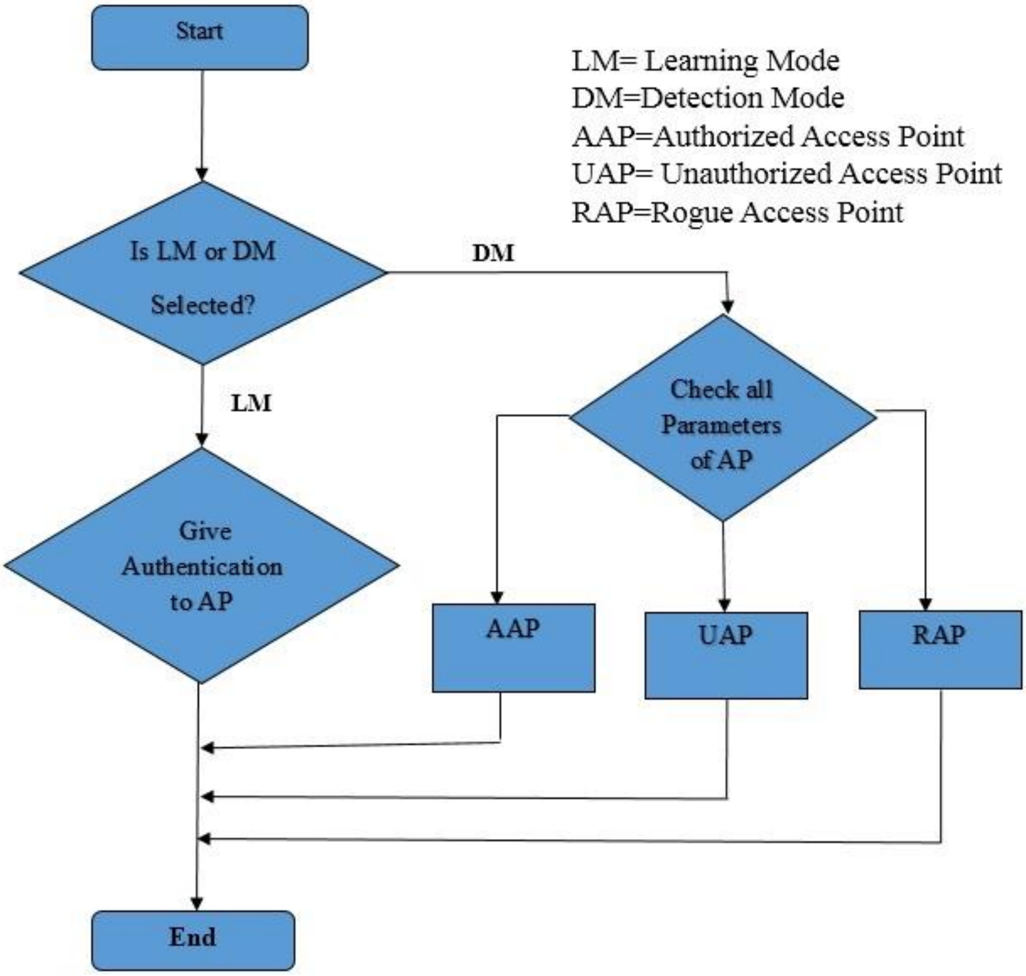

Start
LM= Learning Mode
DM=Detection Mode
AAP=Authorized Access Point
UAP= Unauthorized Access Point
RAP=Rogue Access Point
Is LM or DM Selected?
DM
LM
Check all Parameters of AP
Give Authentication to AP
AAP
UAP
RAP
End

Figure 4.5: Flowchart of RAP Detection Method

4.6 Mathematical Model

Let $A_p = \{a_1, a_2, a_3$ ...an}, where A_p is a set of access points that ranges from 1 to n.

$a_i = \{a_{im}, a_{is}, a_{ic}, a_{it}, a_{ir}, a_{ie}, a_{isc}\}$

Each access point contains different parameters as given in table 4.3:

Table 4.3: Parameter Description

Parameter	Description
a_{im}	MAC address of the i^th access point
a_{ic}	Channel/frequency,
a_{is}	SSID
a_{it}	Timestamp
a_{isc}	Sequence count
a_{ir}	Received signal strength
a_{ie}	Encryption

For Learning Mode,

$W_L = \forall_1^n \{a_{im}, a_{is,}, a_{ic}, a_{it}, a_{if}, a_{ie}, a_{isc}\}$

Where, W_L is the whitelist of authorized access points.

For Detection Mode,

$D_L = \forall \{a_{im}, a_{is}, a_{ic}, a_{it}, a_{ir}, a_{ie}, a_{isc}\}$

Where, D_L is the list of access points detected by the system in the proximity.

Formally,

$$B \setminus A = \{x \in B \mid x \notin A\} \qquad \ldots \qquad (1)$$

The equation 1 represents set minus operation from the set theory.

Hence,

$$D_L \setminus W_L = \{x \in D_L \mid x \notin W_L\} \qquad \ldots \qquad (2)$$

Using equation 2, RAPs can be inferred by the implemented system, if result set of equation 2 is a not an empty set (¬∅).

4.7 Algorithm

Algorithm 1 describes implemented algorithm for detection of RAPs using multiple parameters. It continuously monitors beacon frames on the network. Two threads are created in the implemented system to run the system in learning as well as detection modes.

Input:

W ⇐ Whitelist of Access Points in the network

```
        $A_l$      ⇐ Legitimate Access Point
        $B_N$      ⇐ Beacon frames captured from the network N
Output:
        $CS_{AP}$  ⇐ Clock Skew
        $SCD_{AP}$ ⇐ Sequence Count difference
        $A_{AAP}$  ⇐ Authorized Access Point list
        $R_{AP}$   ⇐ Rogue Access Point list
        $A_{UAP}$  ⇐ Unauthorized Access Point list
Begin
Step 1:
    $B_{N:}$ Beacon frame captured by the system
    $W$: Read whitelist of the access points in the network
Step 2:
      $B_{mac}$ ⇐$B_N$ Extracts MAC address of the sender AP from the beacon frame
      $B_{ch}$ ⇐$B_N$ Extracts channel number of the sender AP from the beacon frame
      $B_{ssid}$ ⇐$B_N$ Extracts SSID of the sender AP from the beacon frame
      $B_{sc}$ ⇐$B_N$ Extracts sequence count the sender AP from the beacon frame
      $B_{enc}$ ⇐$B_N$ Extracts encryption configuration of the sender AP from the beacon
             frame
      $B_{rss}$ ⇐ $B_N$ Extract received signal strength of the sender AP from the beacon
             frame
Step 3: Compare $Bssid$ with $Wssid$
        If not matched then add to rogue AP list and go to Step 1
Step 4: Compare $Bmac$ with $Wmac$
        If not matched then add to rogue AP list and go to Step 1
Step 5: Compare $B_{ch}$ with $W_{ch}$
        If not matched then add to rogue AP list and go to Step 1
Step 6: Compare $B_{enc}$ with $W_{enc}$
        If not matched then add to rogue AP list and go to Step 1
Step 7: Compare $B_{rss}$ with $W_{rss}$
        If not matched then add to rogue AP list and go to Step 1
Step 8: Compare $B_{sc}$ with $W_{sc}$
        If not matched then add to rogue AP list and go to Step 1
```

```
Step 9:  Compare timestamp values
            missedBF = $SCD_{AP}/16$
            predictedTS = prevTS + missedBF * $CS_{AP}$
            If $B_{ts}$ == predictedTS then go to step 9; Else If not matched, then add to rogue
            AP list and go to    step 1
End
```

4.8 Implementation of the Solution

This method is implemented using python on Ubuntu v14.4 operating system. The code first checks for available wireless network interface cards. After identifying the available wireless network interface cards, it uses all of them to identify wireless networks available in the nearby area. It prepares a list of available networks, from the detected wireless network cards in the system; it identifies the wireless network card for monitor mode using the number of available networks on each card. It is based on the capacity of a card to detect more number of networks; a wireless card from the system is selected to work on monitor mode.

Once monitor mode is created, new thread is created using the threading library in python. The newly created thread is used to switch the channel of access point periodically at a certain threshold value. The threshold value used in this project was 0.5 seconds. A whitelist is used that contains a list of access point with information of SSID, MAC address, Channel, RSS and encryption information.

In detection mode, the beacon frame of each AP available in the network is captured and various parameters like SSID, MAC address, RSS, Timestamp, Sequence No, Frequency and Channel are retrieved. Initially, the SSID from the list is verified. If more than one AP with the same SSID is found, then MAC address of the two APs are compared. If the MAC address is also found to be same, then Frequency of the two APs are compared. In the same manner, the Frequency check is followed by channel check, Encryption check, RSS check, Clock Skew check and finally Sequence Count check. This sequence of checking various parameters of the APs having the same SSID is carried on until any single check results into mismatched values.

The RSS is proved to be useful for the detection of RAP. The RSS level between -100 dB to 0 dB is taken, where 0 means that the device is exactly at the place of the detector, while -100 means it is located at a long distance from the detector. If the RSS value of an AP in a network is -40 as stored in the white list, but in the detection mode, the value obtained is -50, it means that the considered APs physical position is changed. The change from -40 to -50 is not big enough to mark the detected AP as RAP. If the RSS value obtained in the detection mode is -90, then the detected AP is marked as rogue, as the change in the RSS value is considerably high. A difference of 50 in RSS level is considered acceptable in this method.

4.9 Use Case Diagram

The purpose of use case diagram shown in figure 4.6, is to capture the dynamic aspect of a system. Use case diagrams are used to gather the requirements of a system including internal and external influences. These requirements are mostly design requirements. When a system is analyzed to gather its functionalities, use cases are prepared and actors are identified.

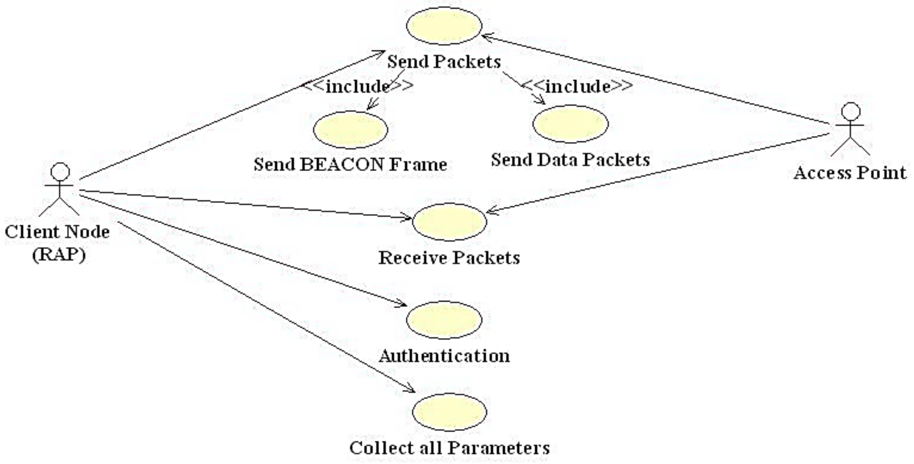


Figure 4.6: Use Case Diagram

4.10 Activity Diagram

Activity diagram as shown in figure 4.7, is basically a flow chart to represent the flow from one activity to another activity. The activity can be described as an operation of the system. The control flow is drawn from one operation to another. This flow can be sequential, branched or concurrent.

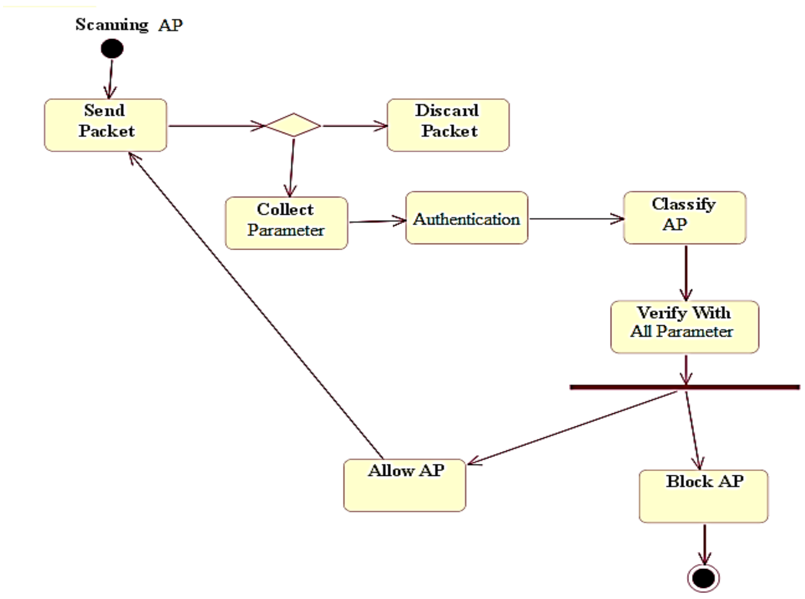


Figure 4.7: Activity Diagram

4.11 Sequence Diagram

Sequence diagram as shown in figure 4.8, emphasizes on time sequence of messages.

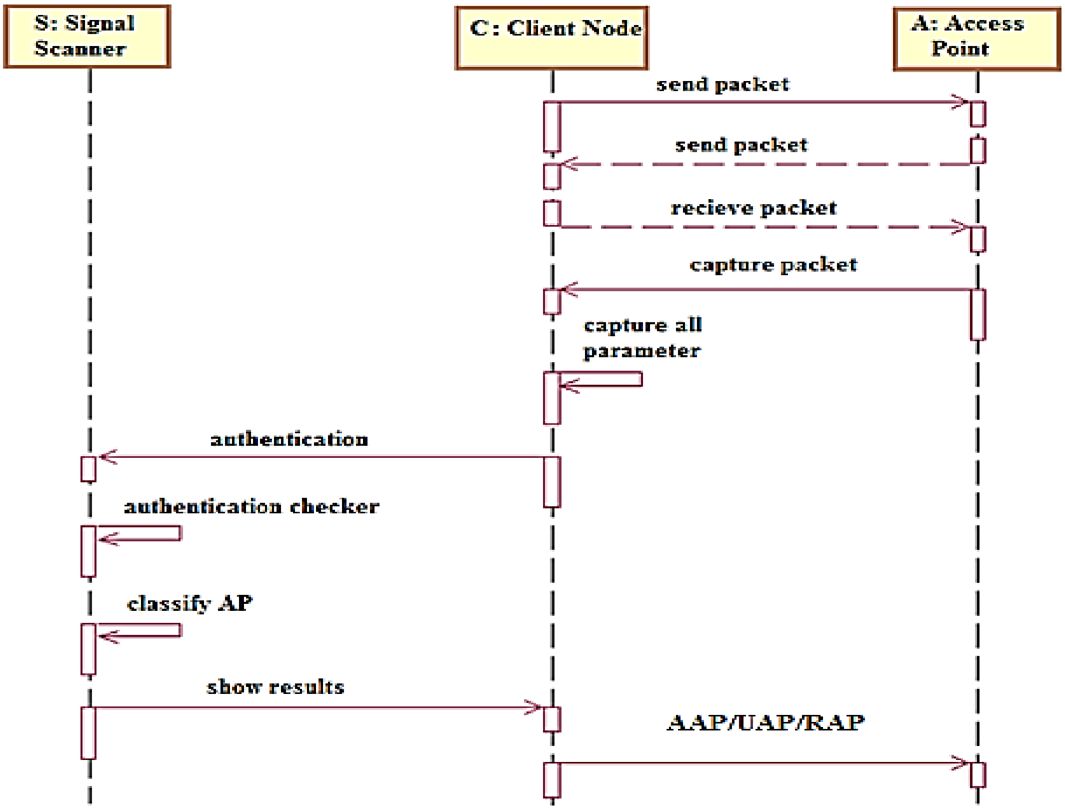


Figure 4.8: Sequence Diagram

4.12 Collaboration Diagram

Figure 4.9 shows the object organization of the collaboration diagram. It shows the method call sequence by using numbering technique. The number indicates how the methods are called one after another.

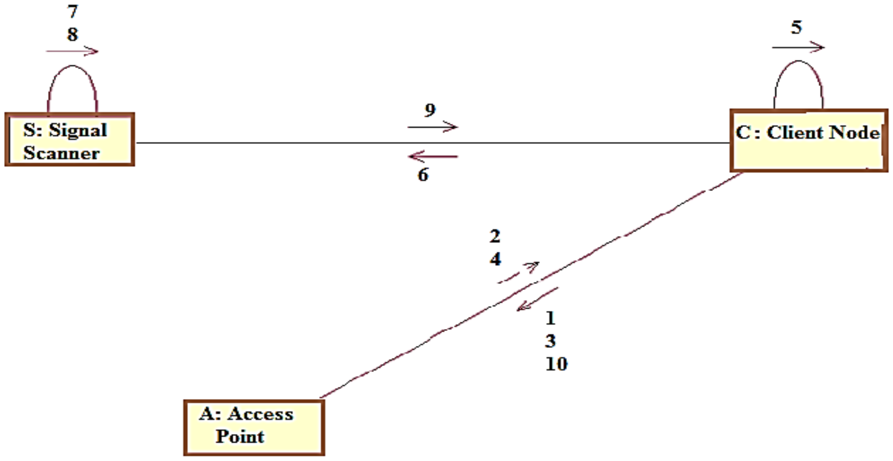


Figure 4.9: Collaboration Diagram

4.13 Deployment Diagram

Deployment diagrams as shown in figure 4.10, are used to visualize the topology of the physical components of a system where the software components are deployed. So, deployment diagrams are used to describe the static deployment view of a system. Deployment diagrams consist of nodes and their relationships.

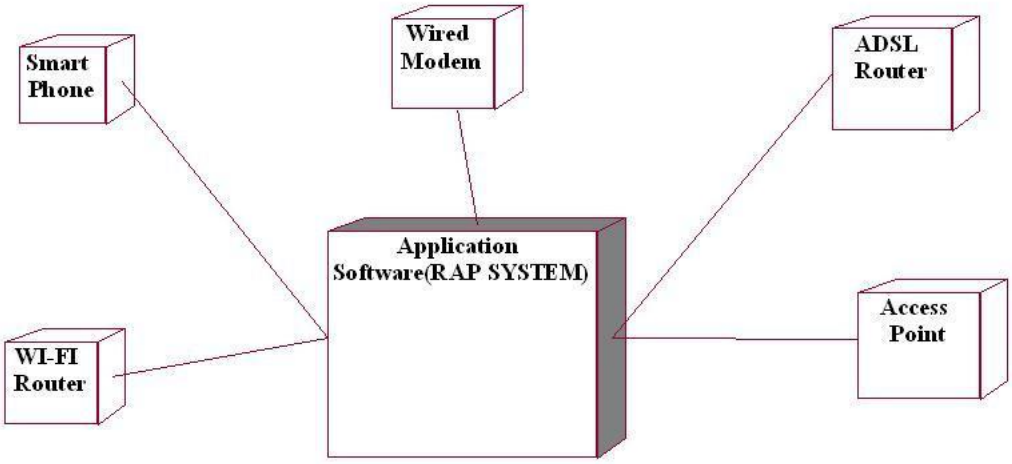


Figure 4.10: Deployment Diagram

4.14 Implementation Environment

4.14.1 Hardware Requirements

Laptop with Intel Core 2 Duo and 2GB RAM

Access Points

Smart Phone

4.15 Software Requirements

4.15.1 Python 2.6

Python is a flexible, independent, powerful and high level language. The python code is robust and easier to understand. Python is used for the following:

- Programming web applications and creating windows applications.
- The network administrator performs daily testing using python for scripting task.
- Developing different web frameworks.

Python helps in supporting large number of packages and modules using different standard libraries. Python contains more than 100 libraries and each of the library have more than 120 modules. General modules help in comparing regular expressions and many mathematical functions. Python also supports network programming, multithreading, and system interface which helps to design and define standard interfaces using protocols such as SMTP, HTTP and FTP with email management capability.

Python provides support to third party software that are freely available.

4.15.2 Scapy 2.1

Scapy library has built in python language. Wireless frames are divided and sniffed using scapy library. Packets are injected, sent and manipulated using scapy library by the user according to the requirements. Scapy sends and captures packets by matching the request which is sent by wireless devices. Scapy also performs scanning tasks particularly unit testing and passive scanning depending on probe request. Scapy can remove and replace any part of the wireless network packet like hping, arpspoof, arping, etc. It can effortlessly handle additional functionalities like injecting 802.11 frames and combing other techniques to complete a particular task. The main tasks of scapy is to send the packets and receive their answers. It allows us to define 802.11 frames and inject them in wireless network.

Scapy discovers the nodes in the network by sending request to all devices in the network and checking their responses with their time-to-live (TTL) value.

4.15.3 Operating System

Linux, Ubuntu / Back track 5, Kali, Redhat Linux.

Redhat Linux- Redhat Linux is most popular linux distribution in open source technologies. It is widely used in enterprise environment for various computing purposes. Hence it is an ideal operating system to test various wireless technologies. Redhat Linux supports TCP/IP network stack and various IEEE standards. This makes it an ideal choice of deployments in last mile networks. It also makes a strong case for using Redhat Linux for testing RAP detection.

Ubuntu- Ubuntu is Debian based Linux distribution widely popular across world for client side computing. It is also used in smartphones and entry level servers. As it supports TCP/IP and other IEEE standards it is very popular in all enterprise networks. It supports large number of wireless devices and wireless technologies. Thus to study the effectiveness of RAP solution it is necessary to study its performance on Ubuntu.

Backtrack: Backtrack is popular Linux distribution used for implementing and testing computer, network and information security. It has wide array of features used by security professionals to perform various penetration testing activities on various applications and systems. It supports vulnerability assessment and penetration testing of various network and wireless technologies such as IEEE standards. Therefore security tester across the world use this distribution for testing wireless technologies. Naturally this tool is preferred choice for studying RAP detection.

Kali Linux: Kali Linux is another Linux distribution that is very popular among security testers. It is Debian based open source project which has strict requirements for any new code to get added in side Linux kernel. This makes is very secure and preferred choice among testers. It is widely used for conducting vulnerability assessments and penetration testing as well as various digital forensic activities. It contains extensive support testing various wireless attack scenarios and hence an ideal choice to study and test RAP detection.

CHAPTER-5

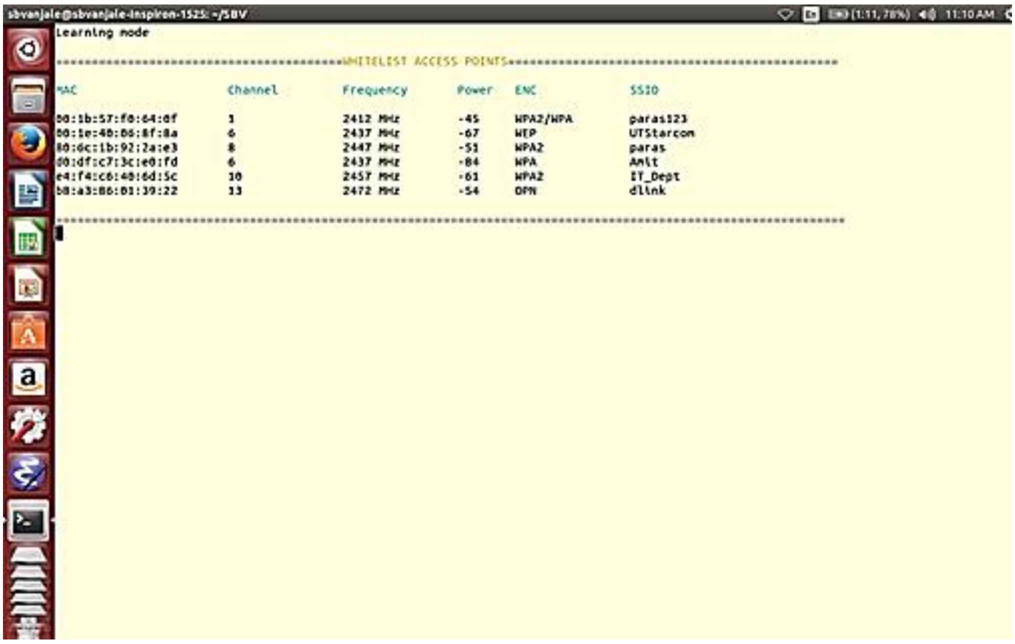
EXPERIMENTAL RESULTS AND ANALYSIS

5.1 TEST CASES

Test Case 1 – Learning Mode

First the program is executed in the learning mode. The APs present in the range of the host machines are stored in white list.

Output: It shows list of all authorized APs present in the network with their SSID, MAC Address, Channel, Frequency, Power, and Encryption Type.



```
Learning mode

****************************************WHITELIST ACCESS POINTS******************************************

MAC                   Channel        Frequency      Power  ENC           SSID

00:1b:57:f0:64:0f     1              2412 MHz       -45    WPA2/WPA      paras123
00:1e:40:06:8f:8a     6              2437 MHz       -67    WEP           UTStarcom
80:6c:1b:92:2a:e3     8              2447 MHz       -51    WPA2          paras
d0:df:c7:3c:e0:fd     6              2437 MHz       -84    WPA           Amit
e4:f4:c6:40:6d:5c     10             2457 MHz       -61    WPA2          IT_Dept
b8:a3:86:01:39:22     13             2472 MHz       -54    OPN           dlink

**********************************************************************************************************
```

Figure 5.1: List of APs present in the network

Test Case 2 – White List

2.1 White list stores all information of authorized APs along with all related parameters and gives authentication to each AP.

paras123 00:1b:57:f0:64:0f 1 -45 WPA2/WPA

UTStarcom 00:1e:40:06:8f:8a 6 -67 WEP

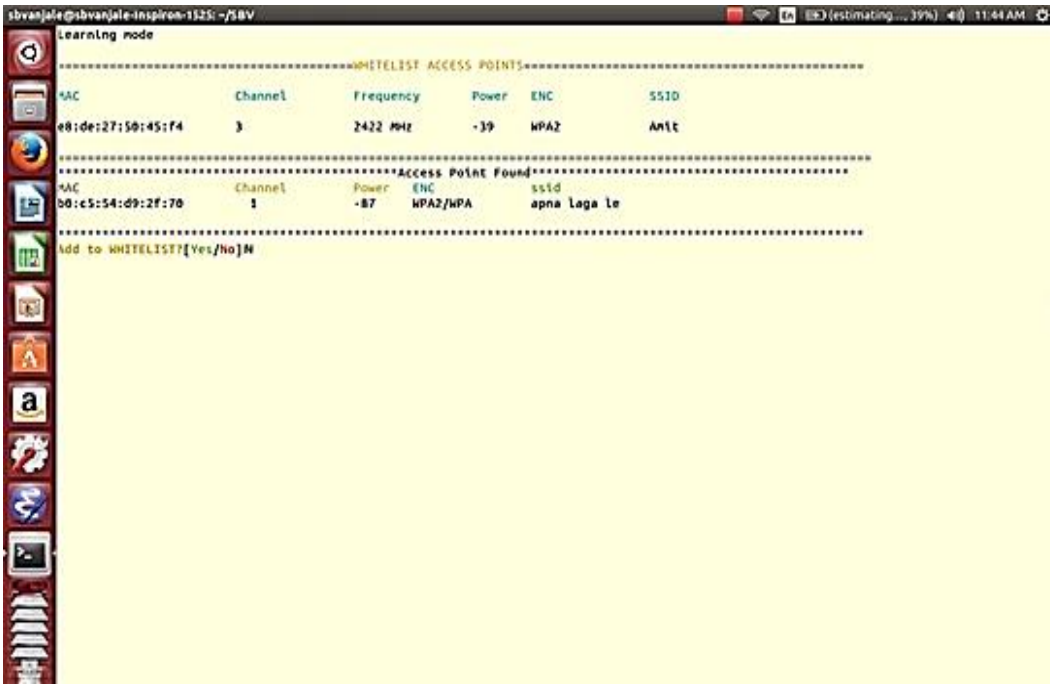
paras 80:6c:1b:92:2a:e3 8 -51 WPA2

Amit d0:df:c7:3c:e0:fd 6 -84 WPA

IT_Dept e4:f4:c6:40:6d:5c 10 -61 WPA2

dlink b8:a3:86:01:39:22 13 -54 OPN

Output: White list text file shown in figure 5.2, gives the list of all authorized APs with their parameters. If ‘Y’ is pressed then that AP is added in whitelist and if ‘N’ is pressed then that AP is shown as unauthorized AP.

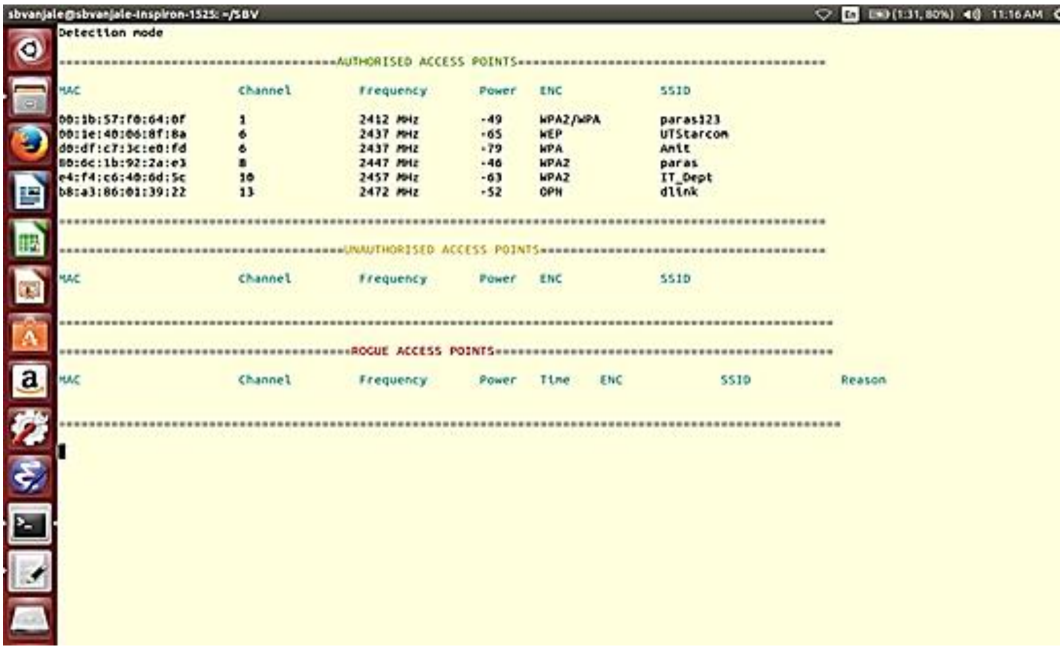


```
Learning mode

***************************************WHITELIST ACCESS POINTS********************************************

MAC                     Channel         Frequency       Power   ENC             SSID

e8:de:27:50:45:f4       3               2422 MHz        -39     WPA2            Amit

************************************************************************************************************
*********************************************Access Point Found*******************************************
MAC                     Channel         Power   ENC             ssid
b0:c5:54:d9:2f:70         1             -87     WPA2/WPA        apna laga le

***********************************************************************************************************
Add to WHITELIST?[Yes/No]N
```

Figure 5.2: White List of APs

Test Case 3- Detection Mode

3.1 Detection mode will detect all APs present in the network.



```
Detection mode

************************************AUTHORISED ACCESS POINTS*****************************************

MAC                     Channel         Frequency       Power   ENC             SSID

00:1b:57:f0:64:0f       1               2412 MHz        -49     WPA2/WPA        paras123
00:1e:40:06:8f:8a       6               2437 MHz        -65     WEP             UTStarcom
d0:df:c7:3c:e0:fd       6               2437 MHz        -79     WPA             Amit
80:6c:1b:92:2a:e3       8               2447 MHz        -46     WPA2            paras
e4:f4:c6:40:6d:5c       10              2457 MHz        -63     WPA2            IT_Dept
b8:a3:86:01:39:22       13              2472 MHz        -52     OPN             dlink

******************************************************************************************************

************************************UNAUTHORISED ACCESS POINTS***************************************

MAC                     Channel         Frequency       Power   ENC             SSID

*******************************************************************************************************

**************************************ROGUE ACCESS POINTS*********************************************

MAC                     Channel         Frequency       Power   Time    ENC             SSID            Reason

********************************************************************************************************
▌
```

Figure 5.3: Detection Mode

Output: Detected APs are classified as Authorized AP, Unauthorized AP and RAP as shown in figure 5.3.

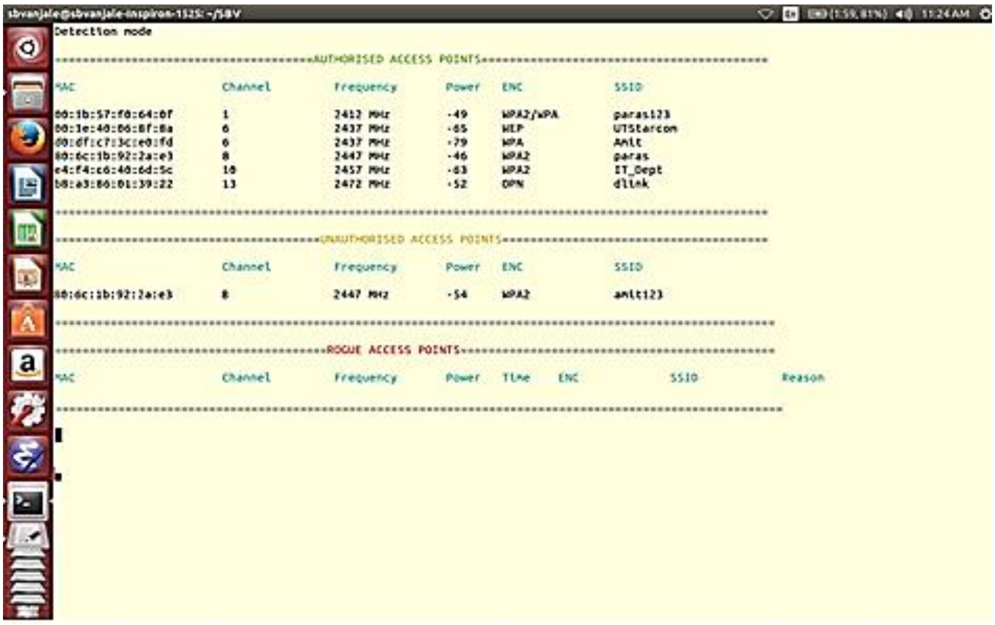
3.2 Detection mode capturing Time Stamp and Sequence Count of Authorized AP.

```
00:1b:57:f0:64:0f  paras123 4747264395 1776 -49 WPA2/WPA 1 2.01520609856
00:1e:40:06:8f:8a  UTStarcom 5264896390 5872 -65 WEP 6 2.05460214615
d0:df:c7:3c:e0:fd   Amit 2221875687 19456 -79 WPA 6 2.06114411354
00:1b:57:f0:64:0f  paras123 4747366791 1792 -53 WPA2/WPA 1 2.12214398384
00:1e:40:06:8f:8a  UTStarcom 5264998792 5888 -64 WEP 6 2.14840817451
d0:df:c7:3c:e0:fd   Amit 2221978088 19472 -79 WPA 6 2.15065908432
00:1b:57:f0:64:0f  paras123 4747469188 1808 -53 WPA2/WPA 1 2.22014117241
00:1e:40:06:8f:8a  UTStarcom 5265101189 5904 -67 WEP 6 2.25095915794
d0:df:c7:3c:e0:fd   Amit 2222080484 19488 -79 WPA 6 2.25480508804
00:1b:57:f0:64:0f  paras123 4747571589 1824 -53 WPA2/WPA 1 2.32598114014
00:1e:40:06:8f:8a  UTStarcom 5265203594 5920 -64 WEP 6 2.35313796997
d0:df:c7:3c:e0:fd   Amit 2222182888 19504 -79 WPA 6 2.35454797745
00:1b:57:f0:64:0f  paras123 4747673989 1840 -53 WPA2/WPA 1 2.42470812798
00:1e:40:06:8f:8a  UTStarcom 5265305995 5936 -64 WEP 6 2.45263409615
d0:df:c7:3c:e0:fd   Amit 2222285279 19520 -78 WPA 6 2.45432114601
00:1b:57:f0:64:0f  paras123 4747776389 1856 -54 WPA2/WPA 1 2.52713108063
00:1e:40:06:8f:8a  UTStarcom 5265408387 5952 -63 WEP 6 2.55507516861
d0:df:c7:3c:e0:fd   Amit 2222387679 19536 -78 WPA 6 2.55649614334
00:1b:57:f0:64:0f   paras123 4747878790 1872 -54 WPA2/WPA 1 2.63294506073
00:1e:40:06:8f:8a   UTStarcom 5265510788 5968 -64 WEP 6 2.66045713425
d0:df:c7:3c:e0:fd    Amit 2222490088 19552 -77 WPA 6 2.66426205635
00:1b:57:f0:64:0f   paras123 4747982304 1904 -54 WPA2/WPA 1 2.73355817795
00:1e:40:06:8f:8a   UTStarcom 5265613189 5984 -64 WEP 6 2.75985217094
00:1b:57:f0:64:0f   paras123 4748083595 1952 -52 WPA2/WPA 1 2.83763098717
00:1e:40:06:8f:8a   UTStarcom 5265715590 6000 -67 WEP 6 2.86548709869
d0:df:c7:3c:e0:fd    Amit 2222694879 19584 -80 WPA 6 2.86922001839
00:1b:57:f0:64:0f   paras123 4748185994 1968 -51 WPA2/WPA 1 2.93668603897
```

Output: Results are stored in Beacon.txt file. It contains sequence count and timestamp of each AP.

Test Case 4- SSID Spoofing

4.1 SSID value of authorized AP is changed.

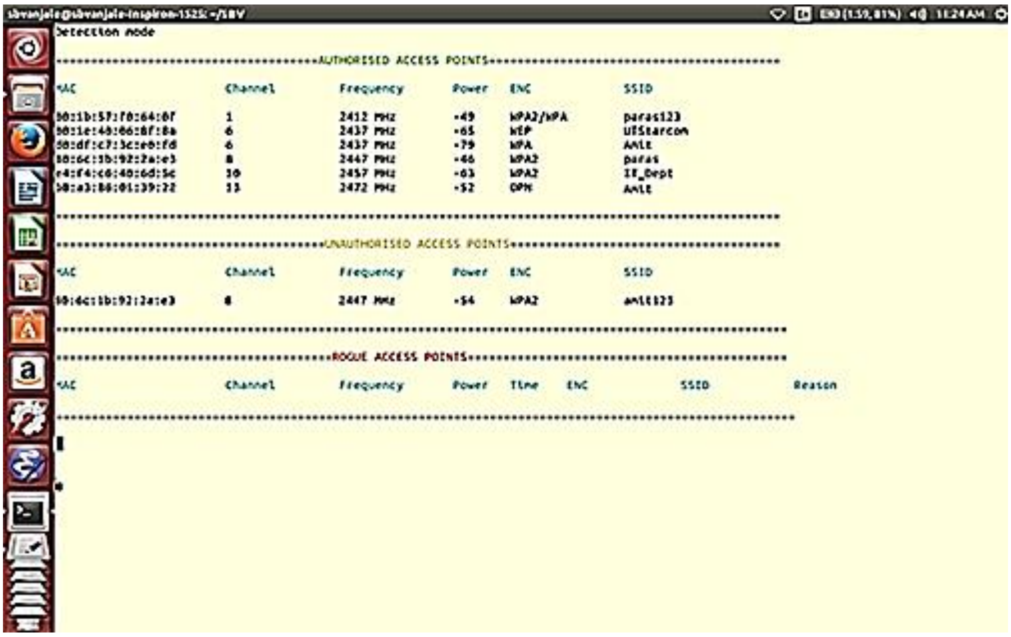


```
sbvanjale@sbvanjale-Inspiron-1525: ~/SBV                                11:24 AM
Detection mode

************************************AUTHORISED ACCESS POINTS****************************************

MAC                    Channel         Frequency       Power   ENC             SSID

00:1b:57:f0:64:0f      1               2412 MHz        -49     WPA2/WPA        paras123
00:1e:40:06:8f:8a      6               2437 MHz        -65     WEP             UTStarcom
d0:df:c7:3c:e0:fd      6               2437 MHz        -79     WPA             Amit
80:6c:1b:92:2a:e3      8               2447 MHz        -46     WPA2            paras
e4:f4:c6:40:6d:5c      10              2457 MHz        -63     WPA2            IT_Dept
b8:a3:86:01:39:22      13              2472 MHz        -52     OPN             dlink

****************************************************************************************************

************************************UNAUTHORISED ACCESS POINTS**************************************

MAC                    Channel         Frequency       Power   ENC             SSID

80:dc:1b:92:2a:e3      8               2447 MHz        -54     WPA2            amit123

****************************************************************************************************

*************************************ROGUE ACCESS POINTS********************************************

MAC                    Channel         Frequency       Power   Time    ENC             SSID            Reason

****************************************************************************************************
```

Figure 5.4: SSID of APs

Output: In detection mode if SSID value of authorized AP is changed then it will become unauthorized AP and will be added to the unauthorized AP list as shown figure 5.4.

4.2 SSID value of authorized AP is changed to a value similar to that of an authorized AP present in white list.

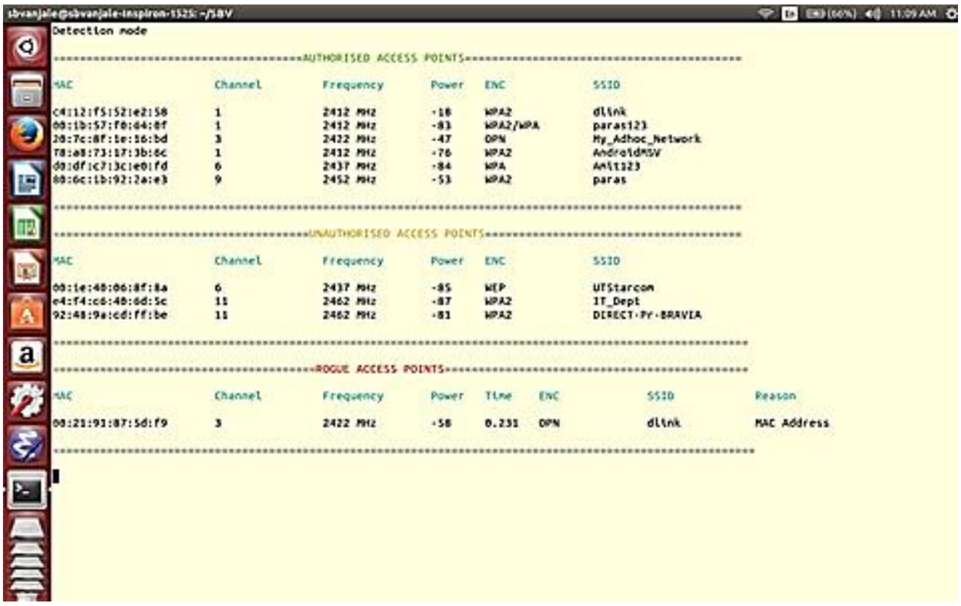


```
sbvanjale@sbvanjale-Inspiron-1525: ~/SBV                                11:24 AM
Detection mode

************************************AUTHORISED ACCESS POINTS****************************************

MAC                    Channel         Frequency       Power   ENC             SSID

00:1b:57:f0:64:0f      1               2412 MHz        -49     WPA2/WPA        paras123
00:1e:40:06:8f:8a      6               2437 MHz        -65     WEP             UTStarcom
d0:df:c7:3c:e0:fd      6               2437 MHz        -79     WPA             Amit
80:6c:1b:92:2a:e3      8               2447 MHz        -46     WPA2            paras
e4:f4:c6:40:6d:5c      10              2457 MHz        -63     WPA2            IT_Dept
b8:a3:86:01:39:22      13              2472 MHz        -52     OPN             Amit

****************************************************************************************************

************************************UNAUTHORISED ACCESS POINTS**************************************

MAC                    Channel         Frequency       Power   ENC             SSID

80:dc:1b:92:2a:e3      8               2447 MHz        -54     WPA2            amit123

****************************************************************************************************

*************************************ROGUE ACCESS POINTS********************************************

MAC                    Channel         Frequency       Power   Time    ENC             SSID            Reason

****************************************************************************************************
```

Figure 5.5: Two authorized APs with same SSID values

Output: In detection mode, there are two APs with same SSID but different MAC addresses, so both these APs will be shown as authorized in figure 5.5.

4.3 SSID value of unauthorized AP is changed to a value similar to that of an authorized AP in white list.



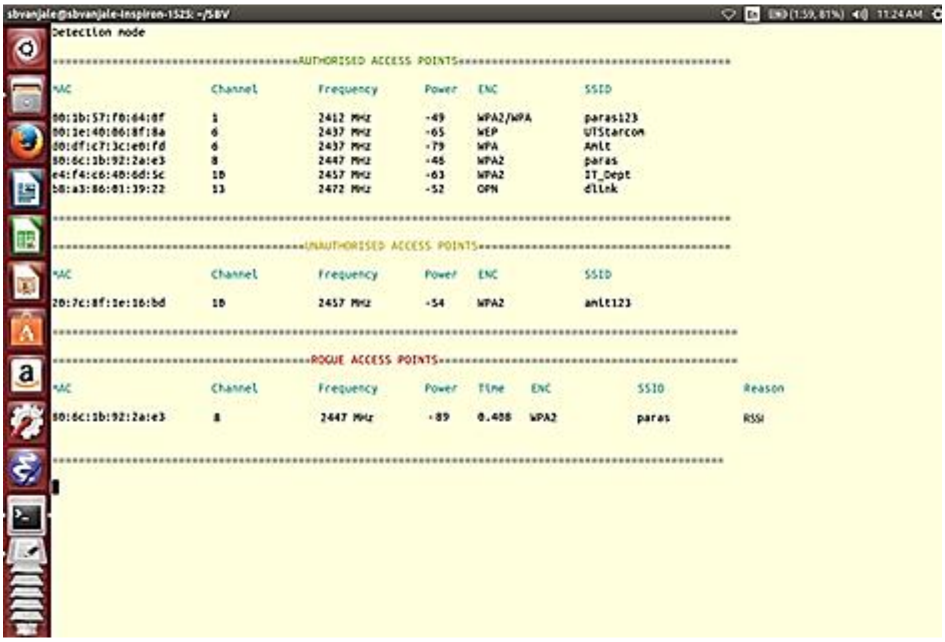
```
Detection mode

*********************************AUTHORISED ACCESS POINTS*********************************

MAC                 Channel       Frequency      Power  ENC             SSID

c4:12:f5:52:e2:58   1             2412 MHz       -18    WPA2            dlink
00:1b:57:f0:d4:0f   1             2412 MHz       -83    WPA2/WPA        paras123
20:7c:8f:1e:56:bd   3             2422 MHz       -47    OPN             My_Adhoc_Network
78:a8:73:17:3b:6c   1             2412 MHz       -76    WPA2            AndroidMSV
d0:df:c7:3c:e0:fd   6             2437 MHz       -84    WPA             Amit123
80:6c:1b:92:2a:e3   9             2452 MHz       -53    WPA2            paras

******************************************************************************************

********************************UNAUTHORISED ACCESS POINTS********************************

MAC                 Channel       Frequency      Power  ENC             SSID

00:1e:40:06:8f:8a   6             2437 MHz       -85    WEP             UTStarcom
e4:f4:c6:40:6d:5c   11            2462 MHz       -87    WPA2            IT_Dept
92:48:9a:cd:ff:be   11            2462 MHz       -81    WPA2            DIRECT-Pr-BRAVIA

******************************************************************************************

***********************************ROGUE ACCESS POINTS************************************

MAC                 Channel       Frequency      Power  Time   ENC             SSID         Reason

00:21:91:87:5d:f9   3             2422 MHz       -58    0.231  OPN             dlink        MAC Address

******************************************************************************************
```

Figure 5.6: SSID Spoofing

Output: The authorized AP with same SSID value, as that of another authorized AP in white list but different MAC address is shown as a RAP in figure 5.6.

Test Case 5 – RAP detection due to difference in RSS values.

5.1 RSS values of all APs are stored in white list.



```
Detection mode

*********************************AUTHORISED ACCESS POINTS*********************************

MAC                 Channel       Frequency      Power  ENC             SSID

00:1b:57:f0:d4:0f   1             2412 MHz       -49    WPA2/WPA        paras123
00:1e:40:06:8f:8a   6             2437 MHz       -65    WEP             UTStarcom
d0:df:c7:3c:e0:fd   6             2437 MHz       -79    WPA             Amit
80:6c:1b:92:2a:e3   8             2447 MHz       -46    WPA2            paras
e4:f4:c6:40:6d:5c   10            2457 MHz       -63    WPA2            IT_Dept
58:a3:86:01:39:22   13            2472 MHz       -52    OPN             dlink

******************************************************************************************

********************************UNAUTHORISED ACCESS POINTS********************************

MAC                 Channel       Frequency      Power  ENC             SSID

20:7c:8f:1e:16:bd   10            2457 MHz       -54    WPA2            amit123

******************************************************************************************

***********************************ROGUE ACCESS POINTS************************************

MAC                 Channel       Frequency      Power  Time   ENC             SSID         Reason

80:6c:1b:92:2a:e3   8             2447 MHz       -89    0.408  WPA2            paras        RSSI

******************************************************************************************
```

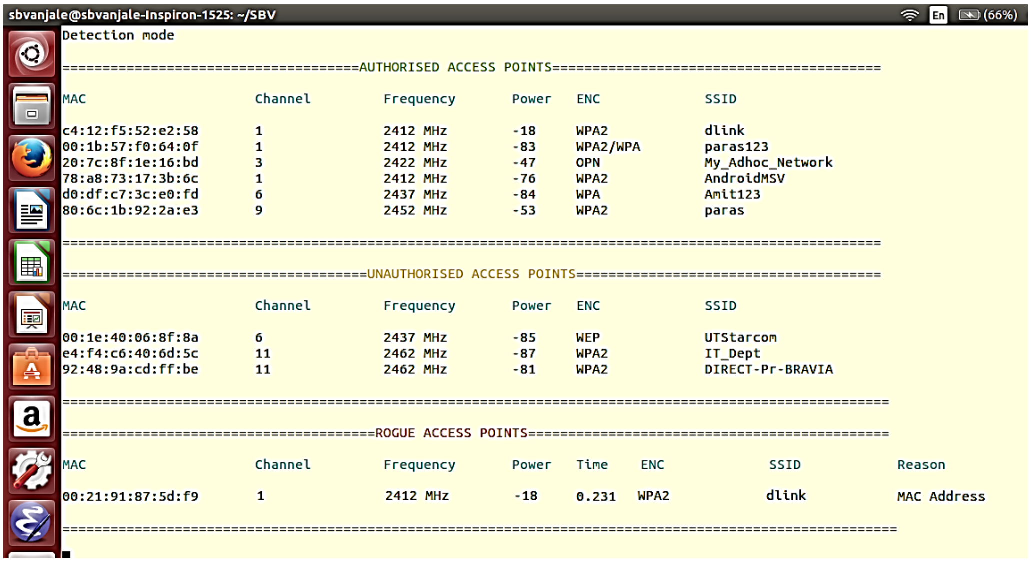
Figure 5.7: RAP Detection due to Difference in RSS values

Output: If the difference of original RSS value and present RSS value has a difference of more than 20, then it will be added to RAP list.

Test Case 6- MAC Address Spoofing

In this case, MAC address spoofing is done.

6.1 MAC address of authorized AP is changed.

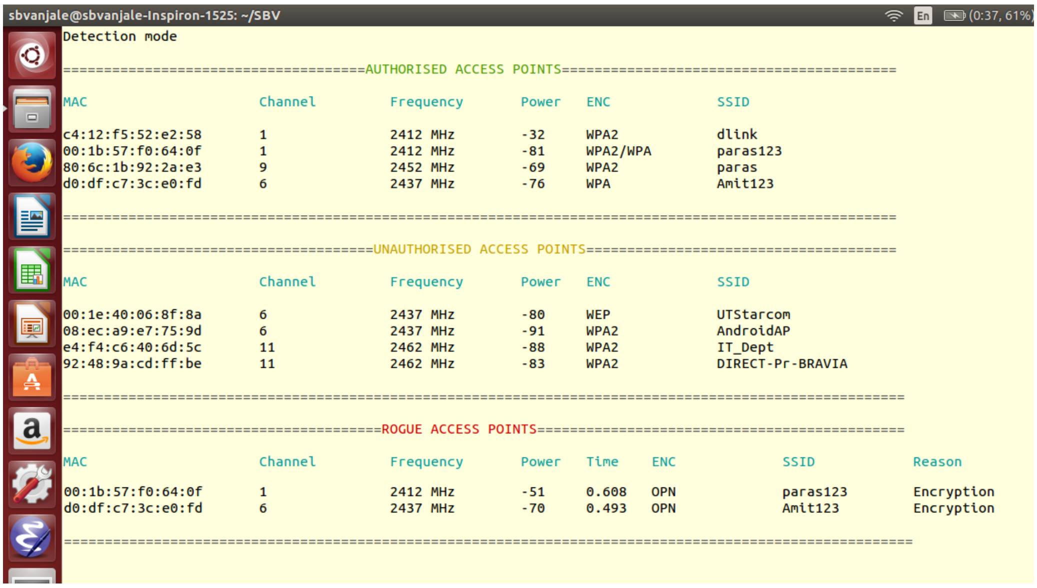


```
Detection mode

=====================================AUTHORISED ACCESS POINTS==========================================

MAC                     Channel         Frequency       Power   ENC             SSID

c4:12:f5:52:e2:58       1               2412 MHz        -18     WPA2            dlink
00:1b:57:f0:64:0f       1               2412 MHz        -83     WPA2/WPA        paras123
20:7c:8f:1e:16:bd       3               2422 MHz        -47     OPN             My_Adhoc_Network
78:a8:73:17:3b:6c       1               2412 MHz        -76     WPA2            AndroidMSV
d0:df:c7:3c:e0:fd       6               2437 MHz        -84     WPA             Amit123
80:6c:1b:92:2a:e3       9               2452 MHz        -53     WPA2            paras

=======================================================================================================

======================================UNAUTHORISED ACCESS POINTS=======================================

MAC                     Channel         Frequency       Power   ENC             SSID

00:1e:40:06:8f:8a       6               2437 MHz        -85     WEP             UTStarcom
e4:f4:c6:40:6d:5c       11              2462 MHz        -87     WPA2            IT_Dept
92:48:9a:cd:ff:be       11              2462 MHz        -81     WPA2            DIRECT-Pr-BRAVIA

========================================================================================================

=======================================ROGUE ACCESS POINTS==============================================

MAC                     Channel         Frequency       Power   Time    ENC             SSID            Reason

00:21:91:87:5d:f9       1               2412 MHz        -18     0.231   WPA2            dlink           MAC Address

=========================================================================================================
```

Figure 5.8: MAC Address Spoofing

Output: In Detection Mode, the authorized AP is shown as RAP because it has different MAC address.

6.2 Unauthorized AP will spoof the SSID and MAC address of authorized AP



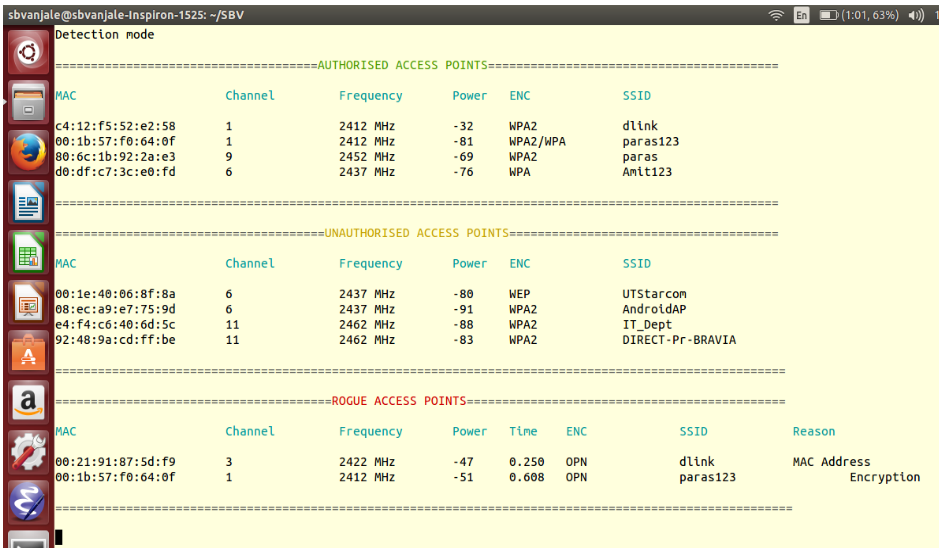
```
Detection mode

=====================================AUTHORISED ACCESS POINTS==========================================

MAC                     Channel         Frequency       Power   ENC             SSID

c4:12:f5:52:e2:58       1               2412 MHz        -32     WPA2            dlink
00:1b:57:f0:64:0f       1               2412 MHz        -81     WPA2/WPA        paras123
80:6c:1b:92:2a:e3       9               2452 MHz        -69     WPA2            paras
d0:df:c7:3c:e0:fd       6               2437 MHz        -76     WPA             Amit123

=======================================================================================================

======================================UNAUTHORISED ACCESS POINTS=======================================

MAC                     Channel         Frequency       Power   ENC             SSID

00:1e:40:06:8f:8a       6               2437 MHz        -80     WEP             UTStarcom
08:ec:a9:e7:75:9d       6               2437 MHz        -91     WPA2            AndroidAP
e4:f4:c6:40:6d:5c       11              2462 MHz        -88     WPA2            IT_Dept
92:48:9a:cd:ff:be       11              2462 MHz        -83     WPA2            DIRECT-Pr-BRAVIA

========================================================================================================

=======================================ROGUE ACCESS POINTS==============================================

MAC                     Channel         Frequency       Power   Time    ENC             SSID            Reason

00:1b:57:f0:64:0f       1               2412 MHz        -51     0.608   OPN             paras123        Encryption
d0:df:c7:3c:e0:fd       6               2437 MHz        -70     0.493   OPN             Amit123         Encryption

=========================================================================================================
```

Figure 5.9: SSID and MAC Address Spoofing

Output: In this case the SSID and MAC address of authorized and unauthorized APs are same but they have different encryption values. Hence, that AP is detected as RAP and the reason for detection is specified as ‘encryption mismatch’.

Test Case 7 – Encryption Type

7.1 Encryption type of authorized AP is changed.



```
Detection mode

=====================================AUTHORISED ACCESS POINTS=========================================

MAC                     Channel         Frequency       Power   ENC             SSID

c4:12:f5:52:e2:58       1               2412 MHz        -32     WPA2            dlink
00:1b:57:f0:64:0f       1               2412 MHz        -81     WPA2/WPA        paras123
80:6c:1b:92:2a:e3       9               2452 MHz        -69     WPA2            paras
d0:df:c7:3c:e0:fd       6               2437 MHz        -76     WPA             Amit123

=======================================================================================================

======================================UNAUTHORISED ACCESS POINTS======================================

MAC                     Channel         Frequency       Power   ENC             SSID

00:1e:40:06:8f:8a       6               2437 MHz        -80     WEP             UTStarcom
08:ec:a9:e7:75:9d       6               2437 MHz        -91     WPA2            AndroidAP
e4:f4:c6:40:6d:5c       11              2462 MHz        -88     WPA2            IT_Dept
92:48:9a:cd:ff:be       11              2462 MHz        -83     WPA2            DIRECT-Pr-BRAVIA

========================================================================================================

=======================================ROGUE ACCESS POINTS=============================================

MAC                     Channel         Frequency       Power   Time    ENC             SSID            Reason

00:21:91:87:5d:f9       3               2422 MHz        -47     0.250   OPN             dlink           MAC Address
00:1b:57:f0:64:0f       1               2412 MHz        -51     0.608   OPN             paras123                Encryption

=========================================================================================================
```

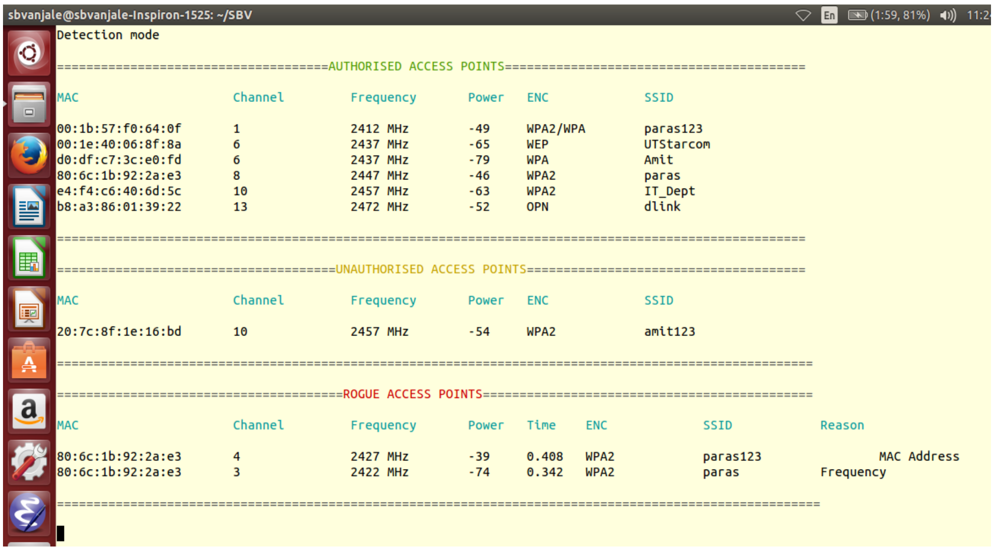
Figure 5.10: Encryption Change

Output: In Detection Mode, the AP with same SSID but different encryption type is detected as RAP.

Test Case 8 –Channel and Frequency

Every channel has a unique frequency. With the change in channel number, its corresponding frequency also changes.

8.1 Access Point is restarted manually or automatically.



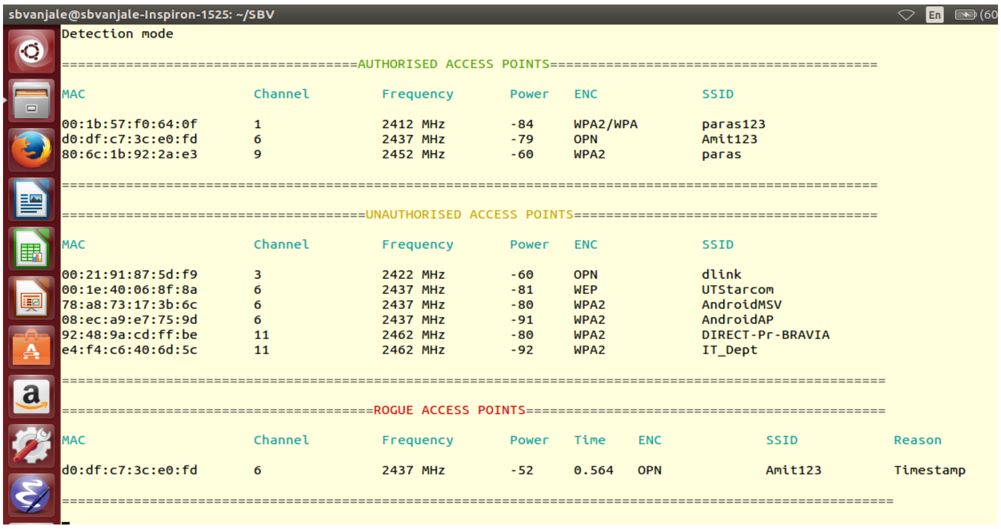
```
sbvanjale@sbvanjale-Inspiron-1525: ~/SBV
Detection mode

=====================================AUTHORISED ACCESS POINTS=========================================

MAC                     Channel         Frequency       Power   ENC             SSID

00:1b:57:f0:64:0f       1               2412 MHz        -49     WPA2/WPA        paras123
00:1e:40:06:8f:8a       6               2437 MHz        -65     WEP             UTStarcom
d0:df:c7:3c:e0:fd       6               2437 MHz        -79     WPA             Amit
80:6c:1b:92:2a:e3       8               2447 MHz        -46     WPA2            paras
e4:f4:c6:40:6d:5c       10              2457 MHz        -63     WPA2            IT_Dept
b8:a3:86:01:39:22       13              2472 MHz        -52     OPN             dlink

======================================================================================================

======================================UNAUTHORISED ACCESS POINTS======================================

MAC                     Channel         Frequency       Power   ENC             SSID

20:7c:8f:1e:16:bd       10              2457 MHz        -54     WPA2            amit123

=======================================================================================================

=======================================ROGUE ACCESS POINTS=============================================

MAC                     Channel         Frequency       Power   Time    ENC             SSID            Reason

80:6c:1b:92:2a:e3       4               2427 MHz        -39     0.408   WPA2            paras123                MAC Address
80:6c:1b:92:2a:e3       3               2422 MHz        -74     0.342   WPA2            paras           Frequency

========================================================================================================
```

Figure 5.11: Channel and Frequency

Output: If SSID and MAC address are same and if AP is restarted manually or automatically. Then it’s Channel and Frequency gets changed, so that authorized AP is detected as RAP.

Test Case 9: Time Stamp and Sequence Count

9.1 SSID, MAC address, Channel and frequency, RSS, and encryption of an AP are spoofed.



```
sbvanjale@sbvanjale-Inspiron-1525: ~/SBV
Detection mode

=====================================AUTHORISED ACCESS POINTS=========================================

MAC                     Channel         Frequency       Power   ENC             SSID

00:1b:57:f0:64:0f       1               2412 MHz        -84     WPA2/WPA        paras123
d0:df:c7:3c:e0:fd       6               2437 MHz        -79     OPN             Amit123
80:6c:1b:92:2a:e3       9               2452 MHz        -60     WPA2            paras

======================================================================================================

======================================UNAUTHORISED ACCESS POINTS======================================

MAC                     Channel         Frequency       Power   ENC             SSID

00:21:91:87:5d:f9       3               2422 MHz        -60     OPN             dlink
00:1e:40:06:8f:8a       6               2437 MHz        -81     WEP             UTStarcom
78:a8:73:17:3b:6c       6               2437 MHz        -80     WPA2            AndroidMSV
08:ec:a9:e7:75:9d       6               2437 MHz        -91     WPA2            AndroidAP
92:48:9a:cd:ff:be       11              2462 MHz        -80     WPA2            DIRECT-Pr-BRAVIA
e4:f4:c6:40:6d:5c       11              2462 MHz        -92     WPA2            IT_Dept

=======================================================================================================

=======================================ROGUE ACCESS POINTS=============================================

MAC                     Channel         Frequency       Power   Time    ENC             SSID            Reason

d0:df:c7:3c:e0:fd       6               2437 MHz        -52     0.564   OPN             Amit123         Timestamp

========================================================================================================
```

Figure 5.12: Time Stamp and Sequence Count

Output: All parameters of the spoofed AP are same as that of an AP in the white list, but its time stamp and sequence count are different. So this spoofed AP is detected as RAP.

5.2 CPU and Primary Memory Utilization before Application Execution:

Figure 5.13 shows the graph for CPU and primary memory utilization. From the graph it is observed that utilization of CPU 1 is 48.5% and that of CPU 2 is 48.0%. The primary memory utilization is seen to be 18.9% before application execution.

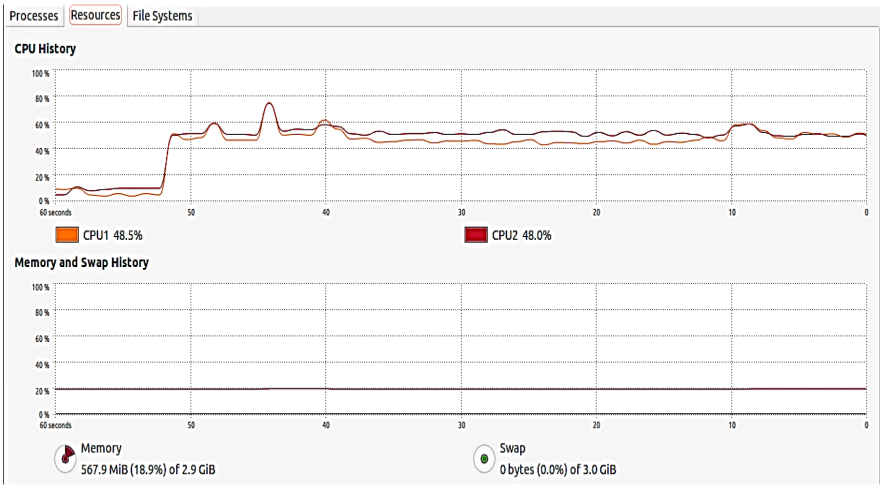


Figure 5.13: Graph for CPU and Primary Memory Utilization before Application Execution

5.3 CPU and Primary Memory Utilization at the Time of Application Execution:

Figure 5.14 shows the graph for CPU and primary memory utilization. From the graph it is observed that utilization of CPU 1 is 51.5%, and that of CPU 2 is 52.5%, while primary memory utilization is 19.1% at the time of application execution.

It is also observed that the primary memory required to run the program is only 16%. This proves that the implemented system has negligible performance overhead in terms of memory utilization.

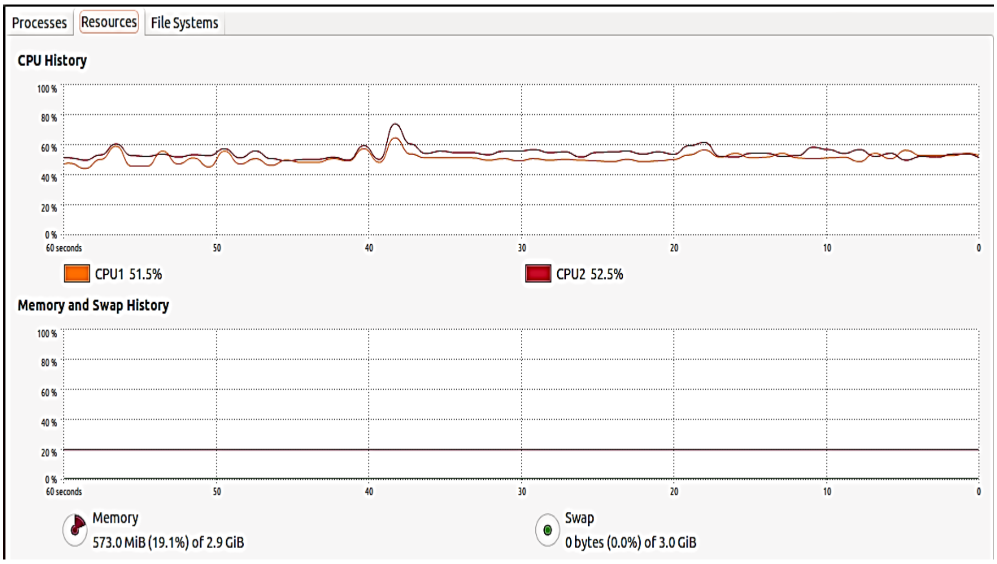


Figure 5.14: Graph for CPU and Primary Memory Utilization at the Time of Application Execution

5.4 EVALUATION

The implemented approach is evaluated with a few examples to ensure that it is able to detect RAP. The runtime overhead of the implemented approach is also measured. All experiments were conducted on an Intel Core 2 Duo 2.58 GHz CPU and 4GB RAM, running on Linux Ubuntu v14.4 platform.

5.4.1 Testing Scenarios

To measure effectiveness of the implemented approach, various scenarios were configured and tested with the presence of implemented approach and RAPs.

Scenario 1 - Rouge Access Point: In this scenario the wireless network in college campus was used. The college network contained 5 wireless access points as shown in table 5.1. One RAP was inserted to test effectiveness of software in detection mode using received signal strength of wireless access point as shown in table 5.2. The RAP was configured using same SSID and channel as that of an authorized access point in the network.

Table 5.1: Authorized access points in the network

SSID	Channel	RSS
Android AP	6	-92
Paras	1	-58
Paras123	11	-90
D-Link	8	-54
Cisco	6	-64

Table 5.2: RAP detection using RSS

SSID	Channel	RSS
Android AP	6	-92
Paras	1	-78
Paras123	11	-90
D-Link	8	-54
Paras	**1**	**-98**
Cisco	6	-64

In detection mode, it was found that an access point with same SSID and channel but different RSS level is present in the network. From these comparisons, the implemented system blocked access point named *Paras* with RSS value equal to -*98*.

Scenario 2 - Evil Twin Attack: Figure 5.15 describes a scenario of Evil Twin access point created in a controlled lab environment using same SSID of legitimate access point. The legitimate access point is shown in the left side of the figure using green color and Evil Twin (malicious) access point is shown in the right side of the figure in red color. The SSID of legitimate access point is ‘Victim’. An Evil Twin access point was created by configuring another access point with the same name ‘Victim’ to attract the users of the victim network. By default the operating system prefers to connect to the known access point that has more signal strength.

The implemented solution easily detected this scenario using MAC address of legitimate access point from whitelist.

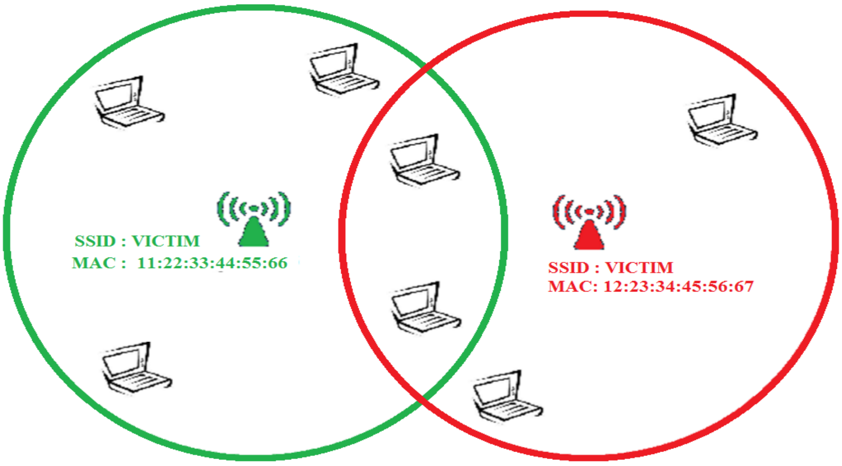


Figure 5.15: Evil Twin with same SSID

Scenario 3 - MAC address spoofing attack: Figure 5.16 describes a scenario of RAP created in a controlled lab environment using various parameters of legitimate access point such as SSID, MAC address, and channel number. The legitimate access point is shown in the left side of the figure using green color and MAC address spoofed RAP is shown in the right side of the figure in red color. The authorized access points in the networks are shown in table 5.3.The SSID of legitimate access point is "Victim", MAC address is 11:22:33:44:55:66 and channel of communication is 6 as shown in table 5.4. A RAP was created by configuring another access point with the same "Victim" name, same MAC address 11:22:33:44:55:66 and same channel number to attract the users of victim network.

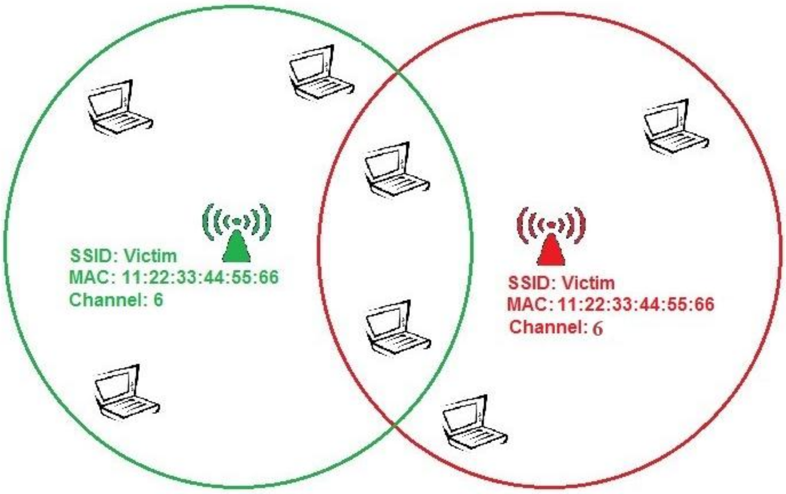


Figure 5.16: SSID and MAC address spoofing attack

The legitimate access point uses encryption to connect to the network. But the RAP does not use encryption as shown in table 5.4. The attacker does not know the passkey of legitimate access point, but if he configures RAP then users would not be able to connect to it, as users do not know what password is set to it. The implemented solution easily detected this attack scenario by detecting the open network used by RAP.

Table 5.3: Authorized access points in the network

SSID	Channel	MAC	Encryption
Victim	6	11:22:33:44:55:66	WPA-PSK
Paras	1	ca:10:7a:39:db:39	WPA-PSK
Paras123	11	f8:1a:67:a1:06:cd	WEP
D-Link	8	52:81:5f:39: 06:cd	WPA-PSK
Cisco	6	06:cd:ad:52:6f:5f	WPA-PSK

Table 5.4: RAP detection using encryption

SSID	Channel	MAC	Encryption
Victim	6	11:22:33:44:55:66	WPA-PSK
Paras	1	ca:10:7a:39:db:39	WPA-PSK
Paras123	11	f8:1a:67:a1:06:cd	WEP
D-Link	8	52:81:5f:39: 06:cd	WPA-PSK
Victim	**6**	**11:22:33:44:55:66**	**OPEN**
Cisco	6	06:cd:ad:52:6f:5f	WPA-PSK

5.5 False Positive and False Negative Rate Detection

To identify the false positive and false negative rate of RAP detection system, war driving technique is used. The war driving was performed in Pune from Katraj to MG road for 10 kilometers. Total 476 wireless networks were detected on the route. These networks were the personal wireless networks setup by the home users or corporates. Two laptops were used for war driving. One was installed with the implemented multi parameter solution and other without the implemented solution. The laptop installed with implemented solution is denoted as ‘L_S’ and the laptop without this solution as ‘L_{US}’. A whitelist of devices on the network was created. Whitelist was not prepared for the wireless network available on the war driving route because the aim was to identify false positive and false negative rate of the system. Therefore, all networks on the route of war driving should get detected as unauthorized access points by the system.

To identify false positive rate and accuracy of the system, verification was performed against the wireless networks detected by the implemented solution on L_S device with the list of wireless networks listed on the L_{US} device. If the number of networks available on the L_{US} device is more than the number of networks listed by L_S then our system has a positive false positive rate. However, it was observed that all the networks identified by L_{US} are listed in unauthorized access points list of the L_S. Thus the war driving analysis shows that the implemented system does not have false positive and false negative rate.

5.6 Performance Overhead

This section comments on the performance overhead of the implemented system in terms of memory utilization and RAP detection time.

5.6.1 Memory Utilization:

To find out memory utilization of the implemented solution, it was tested on three different Linux operating systems, namely Ubuntu, Kali and RedHat. In each operating system the implemented solution was executed under three different scenarios and actual memory utilization was recorded. The memory utilization was recorded before the execution as well as during execution of the implemented system. It was observed that the actual memory utilization during execution of the implemented solution is just 16%, as shown in figure 5.17.

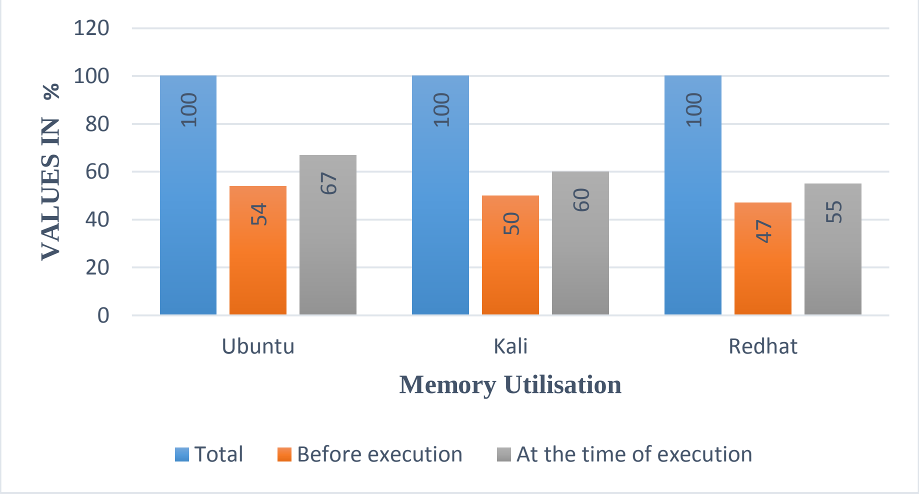


Figure 5.17: Memory utilization during execution of implemented system

5.6.2 Detection Time:

To test the environmental effect on the detection time of implemented system, tests were performed for a period of one week during morning, afternoon and evening time slots. Total 500 beacon frames were captured every day during each slot (morning/afternoon/evening) for analysis. The time taken by the implemented system for detection of unauthorized/rogue/malicious access points was measured in milliseconds and it was average of the time required for 500 beacon frames. Figure 5.18 shows average detection time of the implemented system during morning slot. Figure 5.19 shows average detection time of the implemented system during afternoon slot. Figure 5.20 shows average detection time of the implemented system during evening slot.

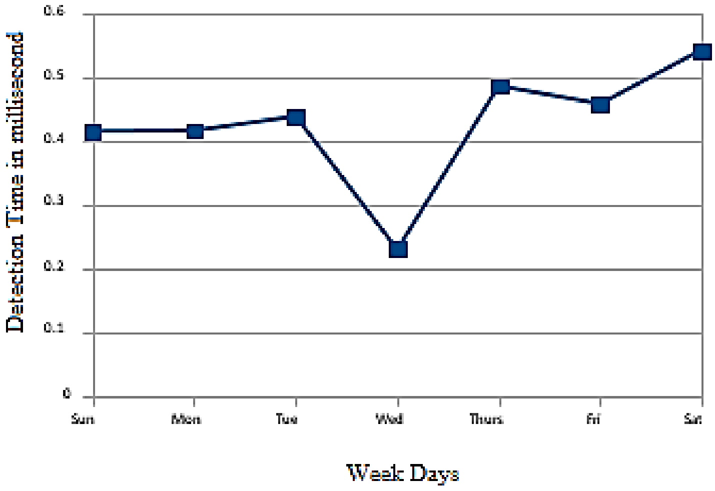


Figure 5.18: Detection Time (milliseconds) of the system over one week period during morning

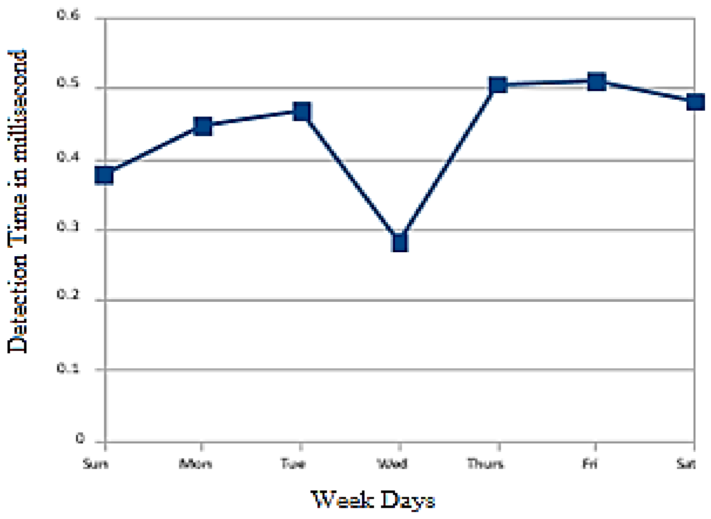


Figure 5.19: Detection Time (milliseconds) of the system over one week period during afternoon

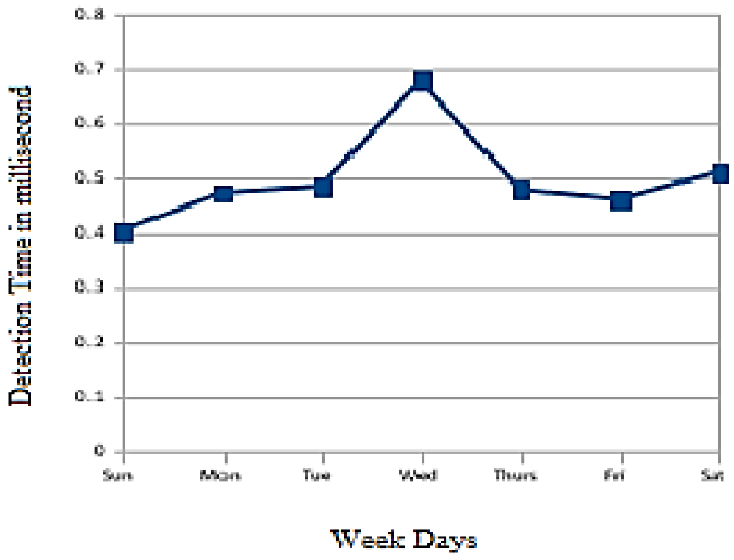


Figure 5.20: Detection Time (milliseconds) of the system over one week period during evening

Table 5.5 provides detection time at three different times in a day for a period of one week, which indicates that there is a slight variation in the detection time of RAP.

Table 5.5: Detection time for 7 days three times in a day

DAY	Detection time (millisecond)		
	Morning	Afternoon	Evening
DAY 1	0.41635071	0.37776568	0.40438871
DAY 2	0.41705828	0.44675744	0.47353369
DAY 3	0.4395086	0.46777152	0.48560363
DAY 4	0.23146203	0.28108175	0.67933706
DAY 5	0.48702937	0.50460719	0.47972569
DAY 6	0.45903486	0.5103086	0.4617354
DAY 7	0.54322756	0.48164336	0.51233516
Average Detection Time(ms)	**0.427667344**	**0.43856222**	**0.499522763**

Table 5.6 shows detection time results of implemented system for RAP detection using MAC address. The detection time without RAP is measured in a safe environment and the detection time with RAP is measured by comparing the MAC address in the network having four nodes and five access points.

Table 5.6: RAP Detection time in milliseconds on the basis of MAC address

Access Points / Nodes	Android AP		Paras		Paras123		D-Link		Cisco	
	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP
Lenovo-1	0.38	0.42	0.36	0.54	0.36	0.38	0.44	0.45	0.30	0.38
Asus-1	0.29	0.34	0.25	0.48	0.24	0.26	0.32	0.36	0.28	0.43
Asus-2	0.42	0.48	0.39	0.41	0.46	0.49	0.49	0.55	0.40	0.46
Dell-1	0.28	0.29	0.27	0.30	0.34	0.50	0.25	0.29	0.32	0.47

Figures 5.21 to 5.25 show the graphs of detection time (msec.) with and without RAP for 5 access points and 4 different nodes for Test Case 1 of MAC address spoofing

attack. It is observed that the detection time with RAP is 17% more than that of without RAP, which is reasonably a minor overhead in detection time.

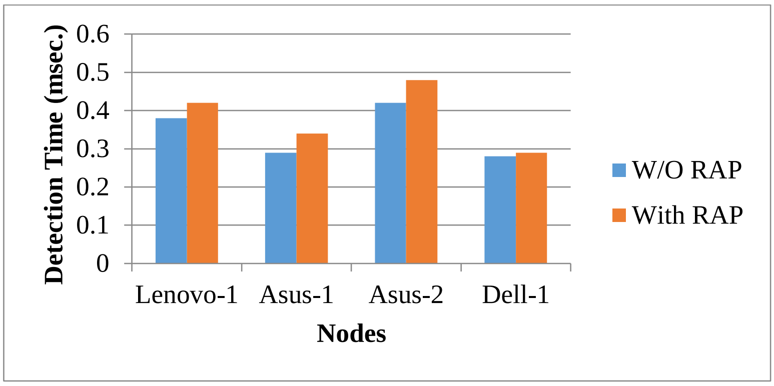


Figure 5.21: Test Case 1 for Access Point: Android AP

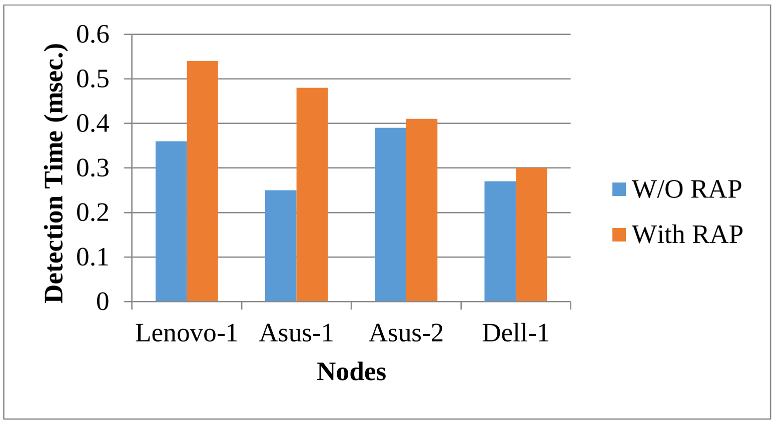


Figure 5.22: Test Case 1 for Access Point: Paras

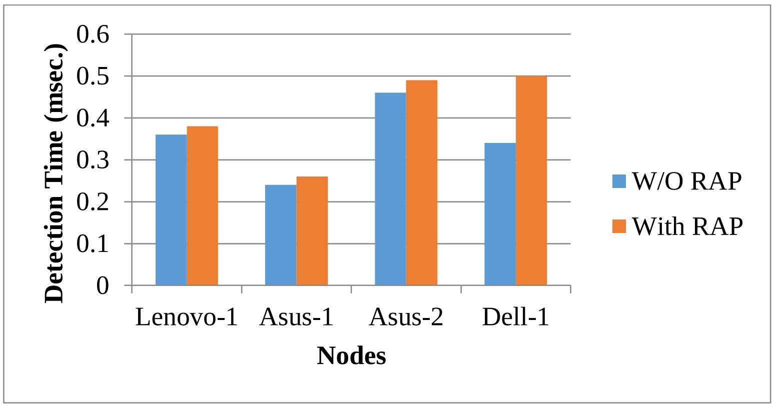


Figure 5.23: Test Case -1 for Access Point: Paras123

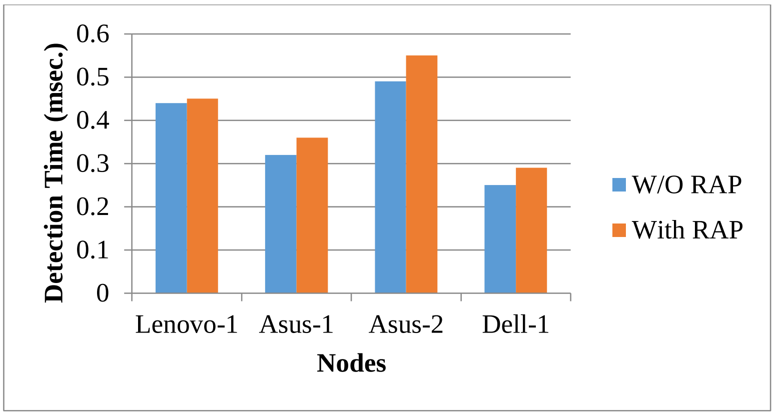


Figure 5.24: Test Case 1 for Access Point: D-Link

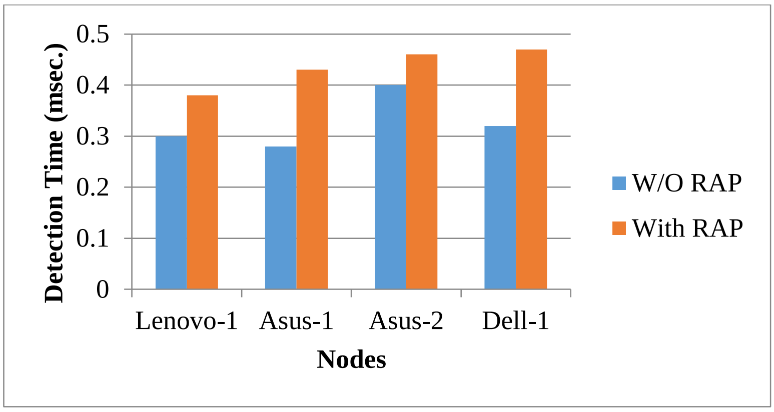


Figure 5.25: Test Case 1 for Access Point: Cisco

Table 5.7 provides detection time for RAP in milliseconds using channel/frequency parameter.

Table 5.8 shows detection time of the implemented system in milliseconds for RAP detection on the basis of encryption mechanism used.

Table 5.9 shows result of the RAP detection time in milliseconds on the basis of received signal strength (RSS).

Table 5.10 shows the result of the implemented system for RAP detection time in milliseconds on the basis of timestamp and sequence count.

Table 5.7: RAP Detection time in milliseconds on the basis of channel/frequency

Access Points / Nodes	Android AP		Paras		Paras123		D-Link		Cisco	
	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP
Lenovo-1	0.43	0.45	0.33	0.43	0.38	0.44	0.43	0.42	0.39	0.43
Asus-1	0.33	0.38	0.21	0.44	0.27	0.35	0.39	0.40	0.32	0.40
Asus-2	0.43	0.46	0.40	0.39	0.36	0.42	0.41	0.60	0.32	0.36
Dell-1	0.27	0.30	0.34	0.38	0.39	0.54	0.33	0.21	0.9	0.44

Figures 5.26 to 5.30 show the graphs of detection time (msec.) with and without RAP for 5 access points and 4 different nodes for test case 2 on the basis of channel/frequency in milliseconds. It is seen from the graphs that the detection time with RAP is increased by approximately 7% as the additional parameter of channel/frequency also takes time for checking.

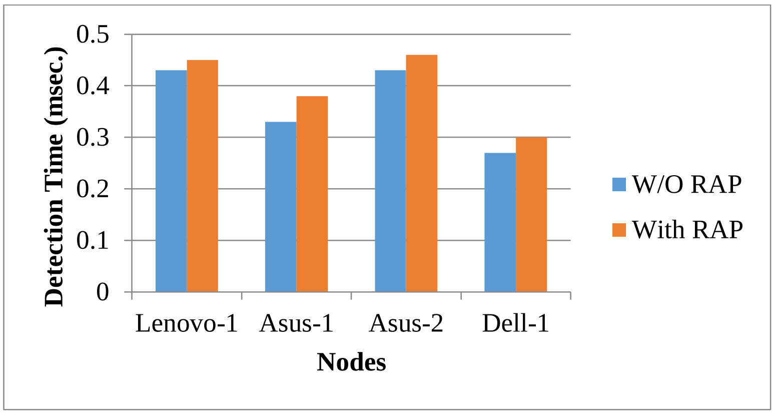


Figure 5.26: Test Case 2 for Access Point: Android AP

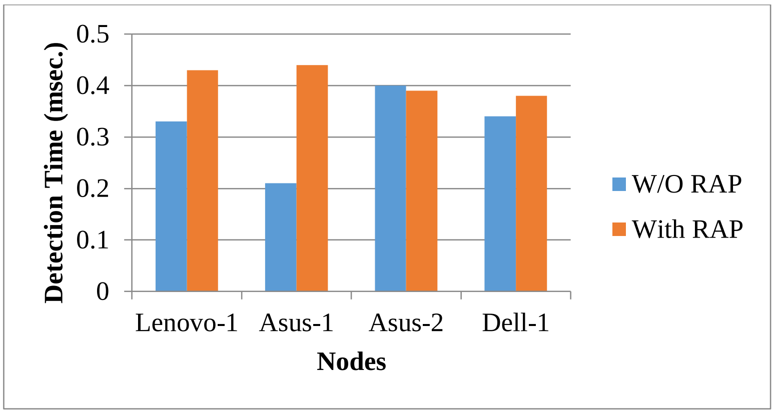


Figure 5.27: Test Case 2 for Access Point: Paras

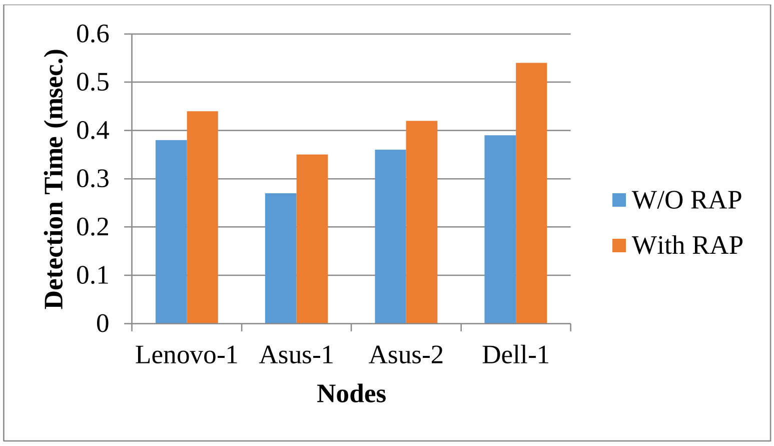


Figure 5.28: Test Case 2 for Access Point: Paras123

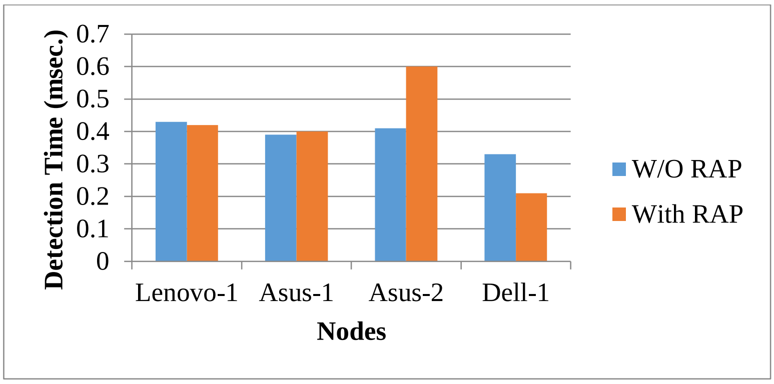


Figure 5.29: Test Case 2 for Access Point: D-Link

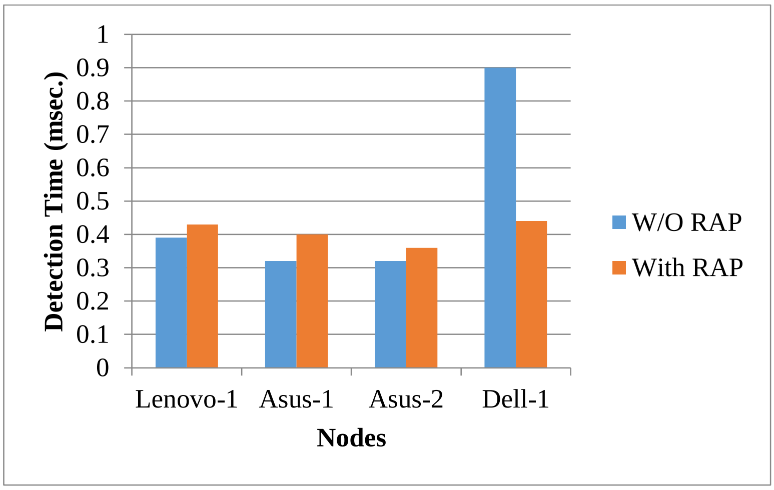


Figure 5.30: Test Case 2 for Access Point: Cisco

Table 5.8: RAP Detection time in milliseconds on the basis of encryption

Access Point / Nodes	Android AP		Paras		Paras123		D-Link		Cisco	
	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP
Lenovo-1	0.42	0.47	0.39	0.41	0.48	0.49	0.33	0.39	0.40	0.45
Asus-1	0.30	0.34	0.25	0.28	0.24	0.30	0.34	0.38	0.27	0.37
Asus-2	0.40	0.42	0.45	0.48	0.49	0.52	0.36	0.48	0.39	0.43
Dell-1	0.24	0.29	0.30	0.34	0.29	0.33	0.38	0.34	0.26	0.38

Figures 5.31 to 5.35 show the graphs of detection time (msec.) with and without RAP for 5 access points and 4 different nodes for Test Case 3 on the basis of encryption in milliseconds. It is seen from the graphs that the detection time with RAP is increased by 11% in these test cases as the additional parameter of encryption also takes time for its checking along with the previous two parameters i.e. MAC address and channel/frequency.

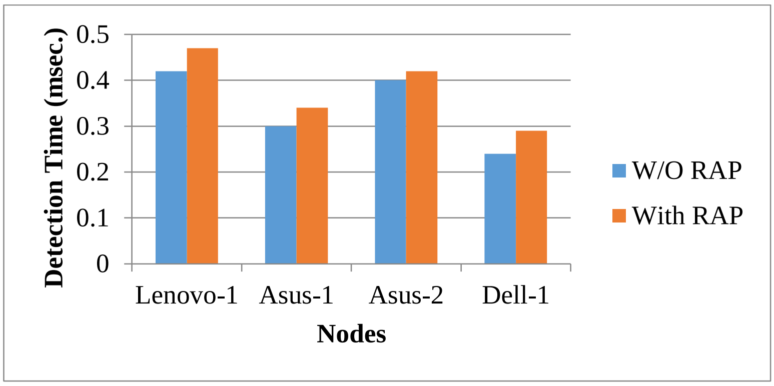


Figure 5.31: Test Case 3 for Access Point: Android AP

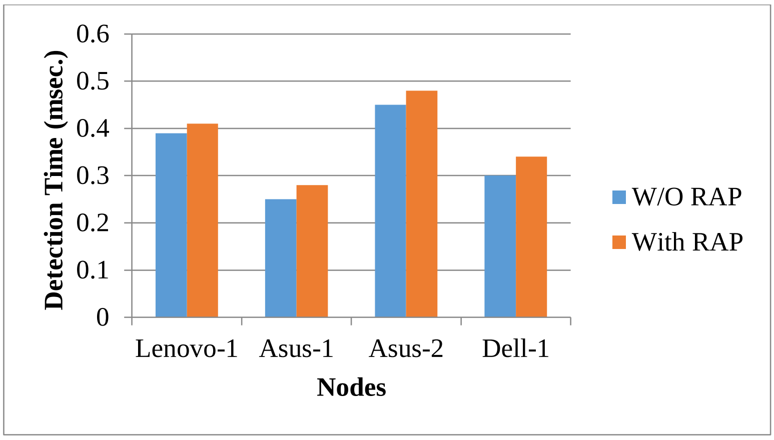


Figure 5.32: Test Case 3 for Access Point: Paras

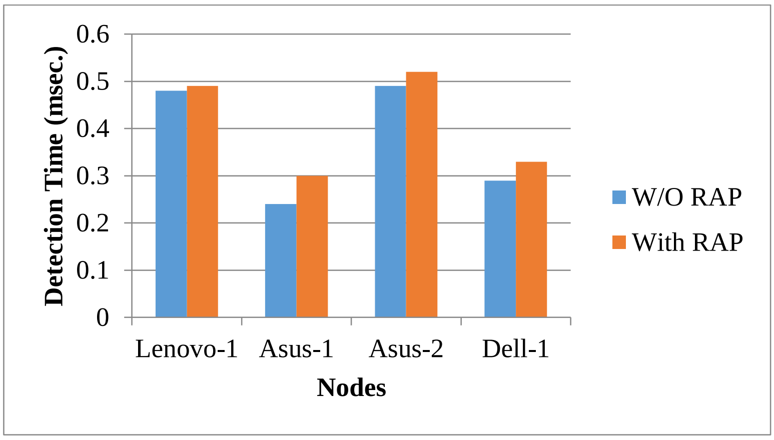


Figure 5.33: Test Case 3 for Access Point: Paras123

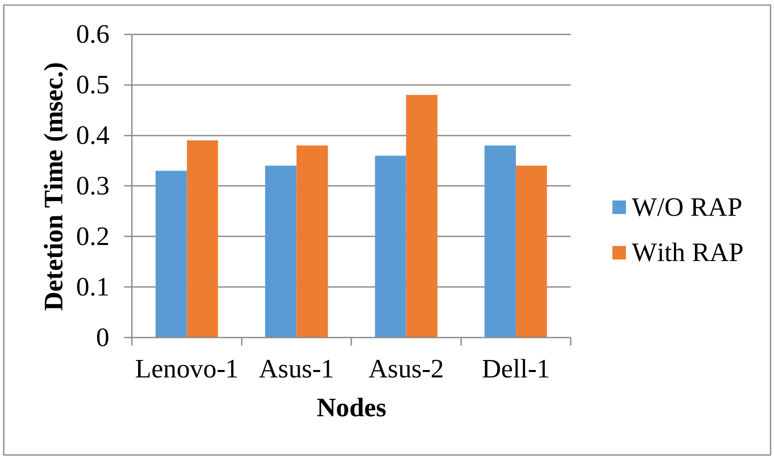


Figure 5.34: Test Case 3 for Access Point: D-Link

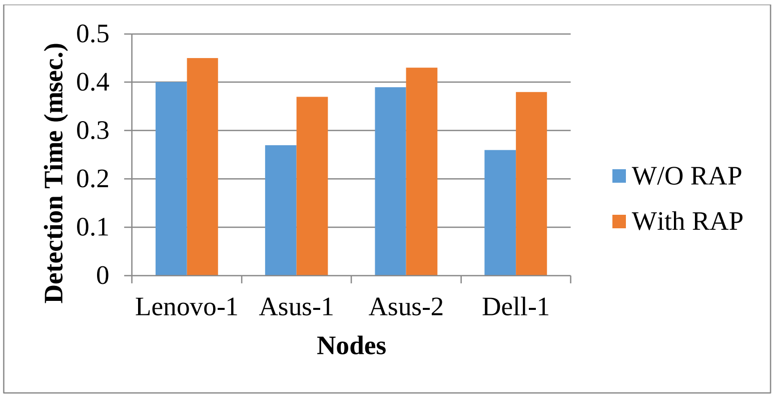


Figure 5.35: Test Case 3 for Access Point: Cisco

Table 5.9: RAP Detection time in milliseconds on the basis of RSS

Access Points / Nodes	Android AP		Paras		Paras123		D-Link		Cisco	
	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP
Lenovo-1	0.54	0.59	0.50	0.57	0.49	0.53	0.44	0.49	0.47	0.56
Asus-1	0.42	0.45	0.43	0.48	0.39	0.48	0.42	0.50	0.40	0.53
Asus-2	0.60	0.58	0.59	0.62	0.54	0.65	0.51	0.58	0.49	0.54
Dell-1	0.29	0.40	0.38	0.39	0.38	0.43	0.48	0.44	0.36	0.48

Figures 5.36 to 5.40 show the graphs of detection time (msec.) with and without RAP for 5 access points and 4 different nodes for Test Case 4 on the basis of RSS in milliseconds. It is seen from the graphs that the detection time with RAP is increased by 11.3 % in these test cases as the additional parameter of encryption also takes time for checking along with previous three parameters i.e. MAC address, channel/frequency and encryption.

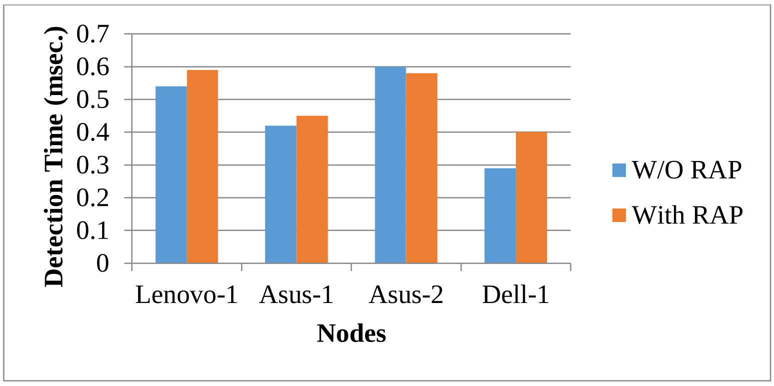


Figure 5.36: Test Case 4 for Access Point: Android AP

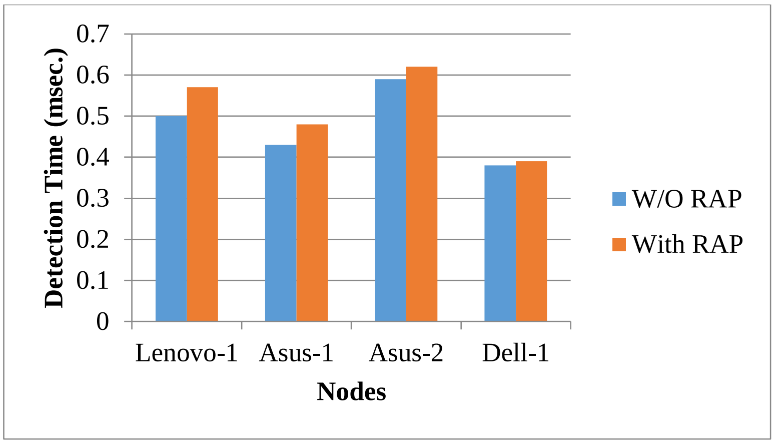


Figure 5.37: Test Case 4 for Access Point: Paras

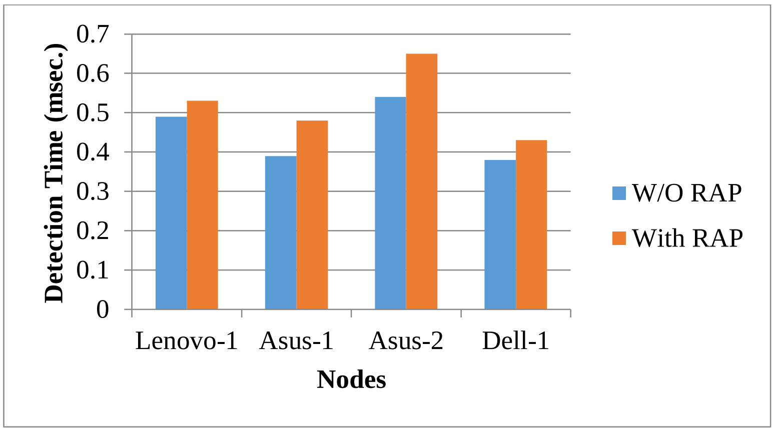


Figure 5.38: Test Case 4 for Access Point: Paras123

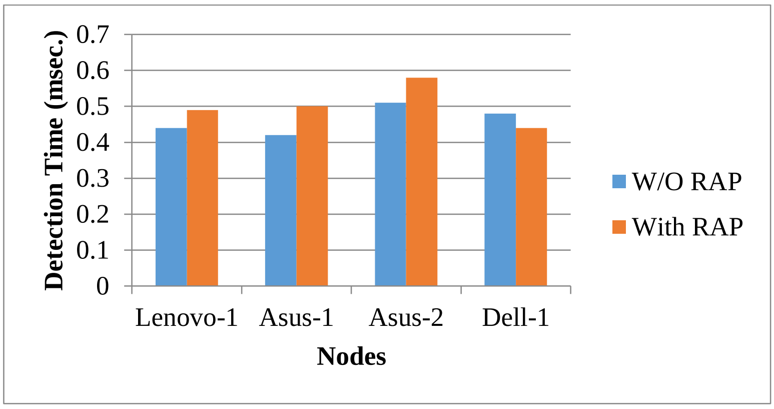


Figure 5.39: Test Case 4 for Access Point: D-Link

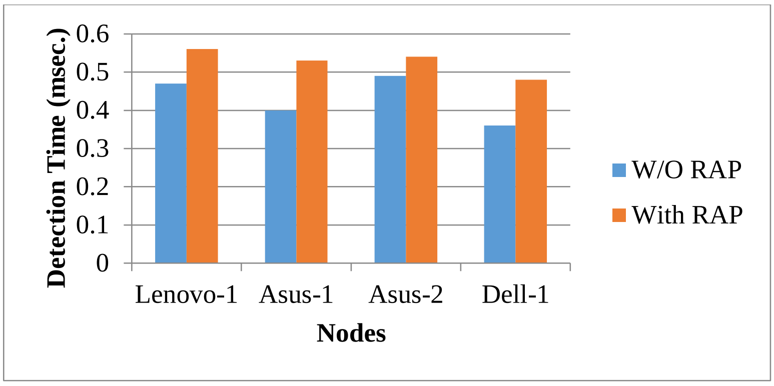


Figure 5.40: Test Case 4 for Access Point: Cisco

Table 5.10: RAP Detection time in milliseconds on the basis of Timestamp and Sequence Count

Access Points / Nodes	Android AP		Paras		Paras123		D-Link		Cisco	
	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP	w/o RAP	with RAP
Lenovo-1	0.44	0.47	0.30	0.47	0.29	0.33	0.30	0.44	0.34	0.40
Asus-1	0.47	0.51	0.44	0.49	0.38	0.41	0.40	0.46	0.30	0.33
Asus-2	0.40	0.38	0.45	0.40	0.29	0.38	0.45	0.38	0.49	0.52
Dell-1	0.30	0.39	0.33	0.34	0.29	0.32	0.34	0.38	0.36	0.40

Figures 5.41 to 5.45 show the graphs of detection time (msec.) with and without RAP for 5 access points and 4 different nodes for Test Case 5 on the basis of Timestamp and Sequence Count in milliseconds. It is seen from the graphs that the detection time with RAP is increased by 10 %.

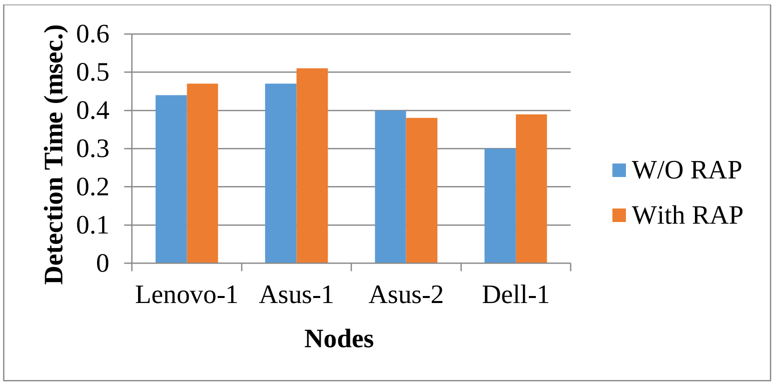


Figure 5.41: Test Case 5 for Access Point: Android AP

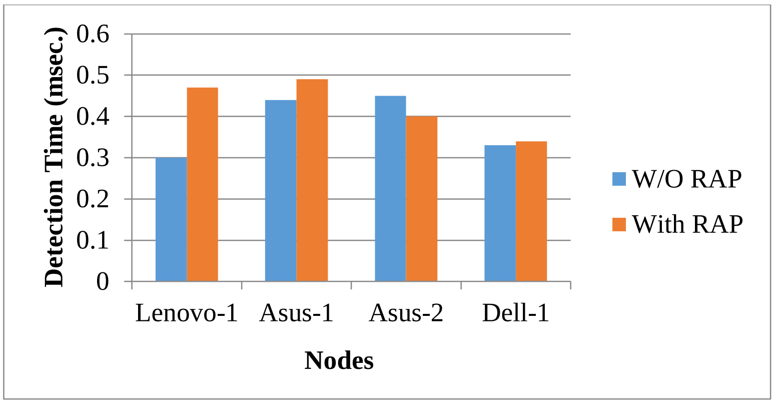


Figure 5.42: Test Case 5 for Access Point: Paras

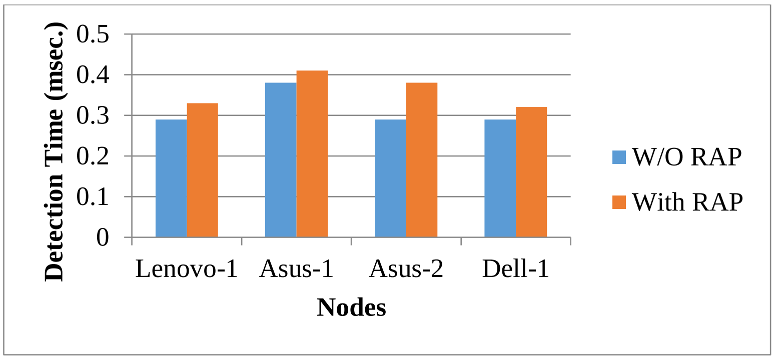


Figure 5.43: Test Case 5 for Access Point: Paras123

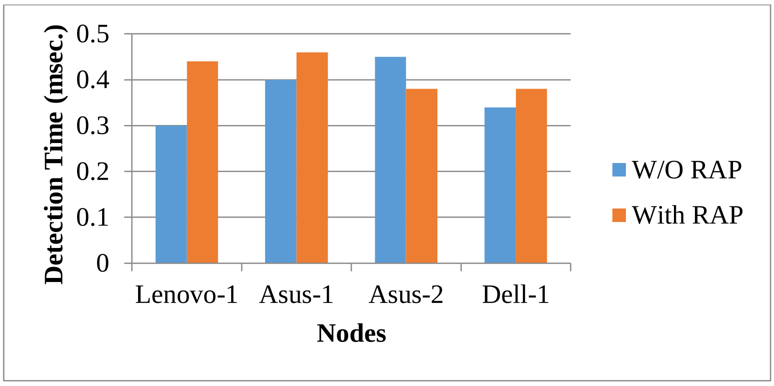


Figure 5.44: Test Case 5 for Access Point: D-Link

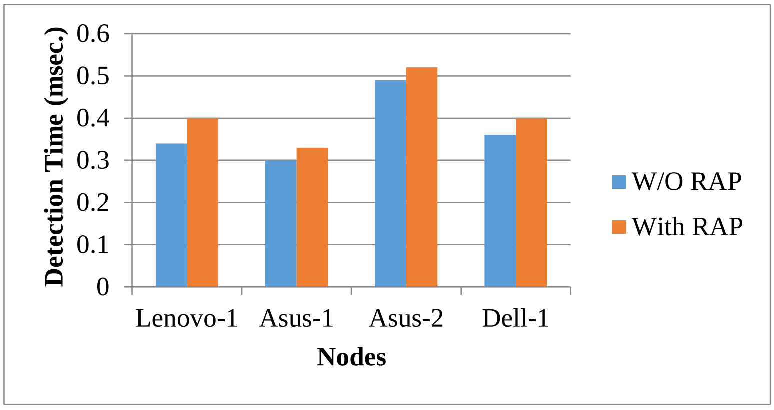


Figure 5.45: Test Case 5 for Access Point: Cisco

5.7 Testing and Analysis

Analysis of testing results is done by using confusion matrix. The entries in the confusion matrix have the following meaning in the context to this research:

- **True Negative (TN)** – **a** is the number of **RAP** detected as **RAP**.
- **False Positive (FP) -** **b** is the number of **RAP** detected as **AAP**.
- **False Negative (FN) - c** is the number of **AAP** detected as **RAP**.
- **True Positive (TP) -** **d** is the number of **AAP** detected as **AAP**.

For the 2 class matrix following standard terms have been defined:

- **Accuracy (AC)** is the proportion of the total number of predictions that were correct. It is determined by using the following equation:

$$\mathbf{AC} = \frac{\mathbf{a+d}}{\mathbf{a+b+c+d}} \dots\dots\dots\dots\dots\ \dots \qquad (1)$$

- **True positive rate (TP)** or **recall** is the proportion of positive cases that were correctly identified and calculated using the following equation:

$$\mathbf{TP} = \frac{\mathbf{d}}{\mathbf{c+d}} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(2)$$

- **False positive rate (FP)** is the proportion of negatives cases that were incorrectly classified as positive, calculated using the following equation:

$$\mathbf{FP} = \frac{\mathbf{b}}{\mathbf{a+b}} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(3)$$

- **True negative rate (TN)** is the proportion of negatives cases that were classified correctly and calculated using the following equation:

$$\mathbf{TN} = \frac{\mathbf{a}}{\mathbf{a+b}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\quad ..(4)$$

- **False negative rate (FN)** is the proportion of positives cases that were incorrectly identified and calculated using the following equation:

$$\mathbf{FN} = \frac{\mathbf{c}}{\mathbf{c+d}} \qquad (5)$$

- **Precision (P)** is the proportion of the predicted positive cases that were correctly identified.

$$\mathbf{P} = \frac{\mathbf{d}}{\mathbf{b+d}} \qquad (6)$$

Test Case 1: SSID and MAC Spoofing

In this case SSID and MAC address of APs are compared with values stored in white list. If SSID of AP is same as that of any of the APs in whitelist then its MAC address is checked. If MAC address is also found to be same, then the corresponding AP is detected as an AAP but if the MAC address is different then it will be detected as RAP.

Table 5.11: Confusion matrix for test case 1

No. of APs	a	b	c	d
10	1	0	1	8
15	2	0	1	12
20	3	0	1	16

Table 5.12: Analysis of test case 1

No. of APs	Accuracy %	TPR %	FNR %	FPR %	TNR %	Precision %
10	90	89	11	0	100	100
15	93.33	92.31	7.69	0	100	100
20	95	94.12	5.88	0	100	100
Average	**92.77**	**91.81**	**8.19**	**0**	**100**	**100**

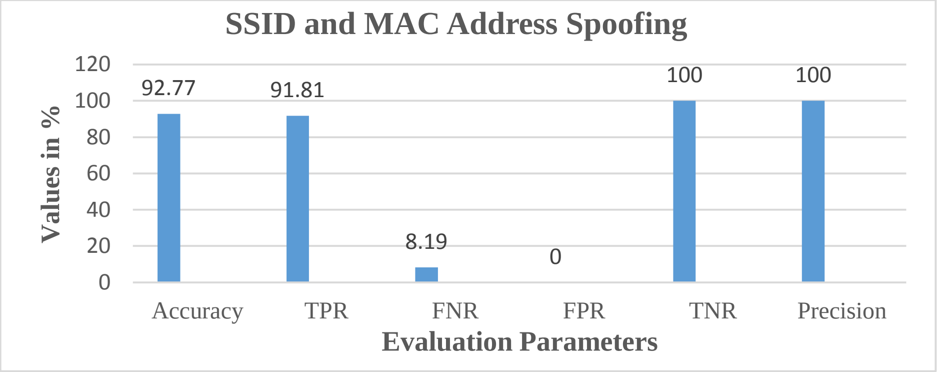


Figure 5.46: Graph for Confusion Matrix of Test Case 1

From the analysis in table 5.11, it is observed that as the number of APs increases the accuracy and true positive rate increases and false negative rate decreases.

The graph in figure 5.46 shows that the average accuracy of RAP detection is 91.11 % when the number of nodes are increased from 10 to 15 and then 20. At the same time the false negative rate is 8.82% which is quite a low value, which further assures better accuracy of the system.

Test Case 2: Channel and Frequency

In this case, the channel and frequency of APs are checked with the values stored in white list. If channel and frequency of AP are same as that of any of the APs in whitelist, then the corresponding AP is detected as an AAP else it will be detected as RAP. Tables 5.13 and 5.14 show the confusion matrix for test case 2 and corresponding values of parameters after analysis, respectively.

Table 5.13: Confusion matrix for test case 2

No. of APs	a	b	c	d
10	1	0	1	8
15	3	0	1	11
20	4	0	1	15

Table 5.14: Analysis of test case 2

No. of APs	Accuracy %	TPR %	FNR %	FPR %	TNR %	Precision %
10	90	89	11	0	100	100
15	93.33	91.67	8.33	0	100	100
20	95	93.75	6.25	0	100	100
Average	**92.77**	**91.47**	**8.53**	**0**	**100**	**100**

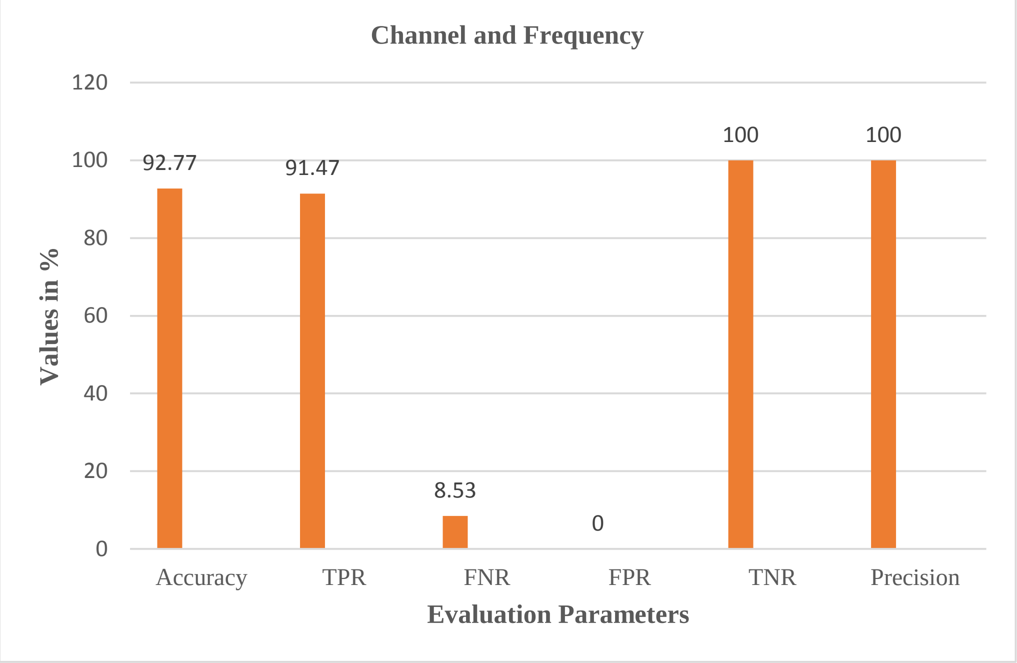


Figure 5.47: Graph for Confusion Matrix of Test Case 2

The graph in figure 5.47 shows that the average accuracy of RAP detection is 92.77 % when the number of nodes are increased from 10 to 15 and then 20. At the same time the false negative rate is 8.19% which is quite a low value, and further assures the better accuracy of the system.

Test Case 3: Encryption Type

In this case the encryption type of access points is checked with the values stored in white list. If encryption type of AP is same as that of any of the APs in whitelist then the corresponding AP is detected as an AAP else it will be detected as RAP. Tables

5.15 and 5.16 show the confusion matrix for test case 3 and corresponding values of parameters after analysis, respectively.

Table 5.15: Confusion matrix for test case 3

No. of APs	a	b	c	d
10	1	0	1	8
15	3	0	1	11
20	5	0	2	13

Table 5.16: Analysis of test case 3

No. of APs	Accuracy %	TPR %	FNR %	FPR %	TNR %	Precision %
10	90	88.88	11.11	0	100	100
15	93.33	91.67	8.33	0	100	100
20	90	86.66	13.33	0	100	100
Average	**91.11**	**89.07**	**10.92**	**0**	**100**	**100**

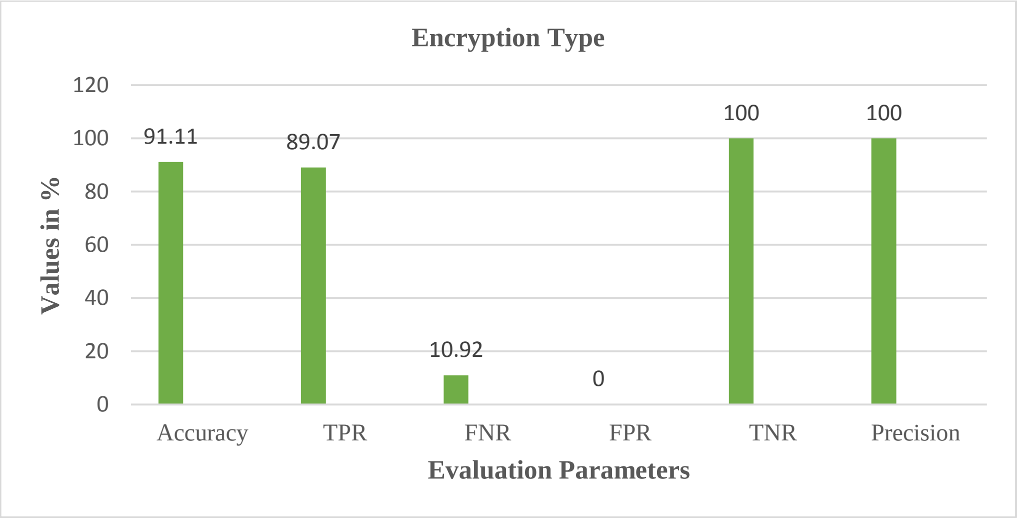


Figure 5.48: Graph for Confusion Matrix of Test Case 3

The graph in figure 5.48 shows that the average accuracy of RAP detection is 91.11 % when the number of nodes are increased from 10 to 15 and then 20. At the same time the false positive rate is 0% which shows the effectiveness of the system.

Test Case 4: Timestamp and Sequence Count

In this case the timestamp and sequence count of access points is checked with the values stored in white list. If timestamp and sequence count of AP is same as that of any of the APs in whitelist then the corresponding AP is detected as an AAP else it will be detected as RAP. Tables 5.17 and 5.18 show the confusion matrix for test case 4 and corresponding values of parameters after analysis, respectively.

Table 5.17: Confusion matrix for test case 4

No. of APs	a	b	c	d
10	2	0	2	6
15	2	0	2	11
20	3	0	2	15

Table 5.18: Analysis of test case 4

No. of APs	Accuracy %	TPR %	FNR %	FPR %	TNR %	Precision %
10	80	75	25	0	100	100
15	86.66	84.61	15.38	0	100	100
20	90	88.23	11.76	0	100	100
Average	**85.55**	**82.61**	**17.38**	**0**	**100**	**100**

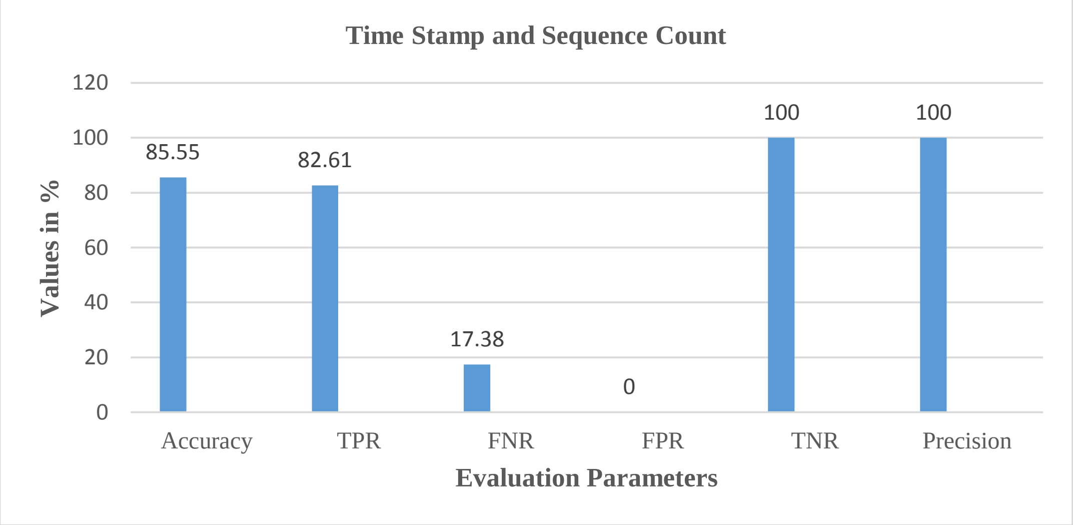


Figure 5.49: Graph for Confusion Matrix of Test Case 4

The graph in figure 5.49 shows that the average accuracy of RAP detection is 85.56 % when the number of nodes are increased from 10 to 15 and then 20. At the same time the false positive rate is 0%, which shows the effectiveness of the system with precision 100%. Figure 5.50 shows the combined graph of all four attack scenarios average values using confusion matrix.

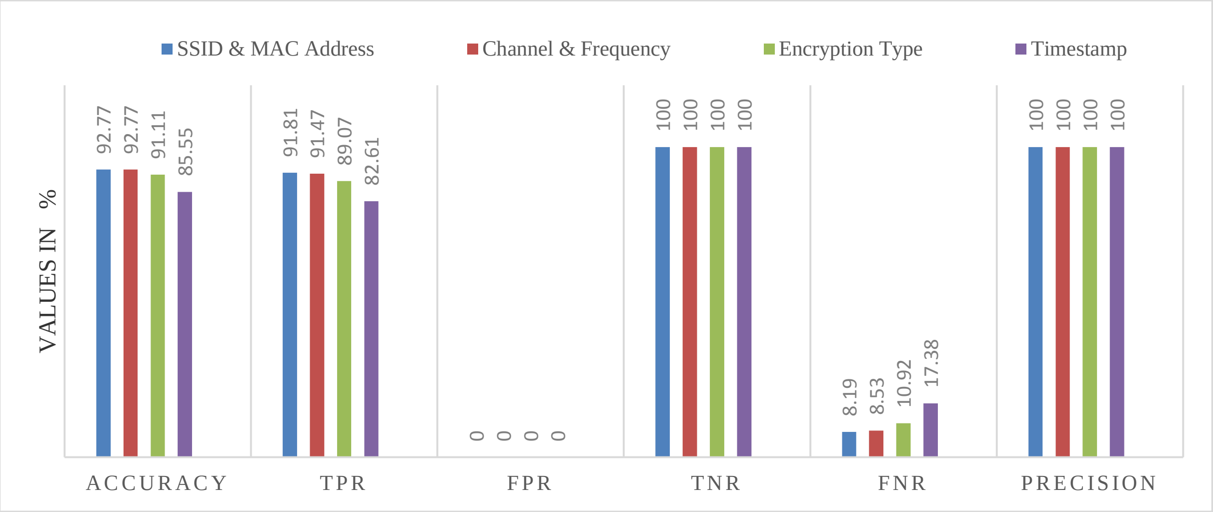


Figure 5.50: Average of All Test Cases

5.8 Results Discussion

5.8.1 Interpreting Experimental Results

In this research work a robust RAP detection technique is developed by integrating multiple parameters into one solution. Use of sequence count and timestamp as an additional parameter for RAP detection is the main contribution of the implemented algorithm. Table 5.19 shows the average values of the evaluation parameters for Test Cases 1 to 4.

Table 5.19: Average Evaluation Parameters for Test Cases 1 to 4

Test Case Scenarios	Accuracy %	TPR %	FNR %	FPR %	TNR %	Precision %
SSID and MAC address spoofing	**92.77**	**91.81**	**8.19**	**0**	**100**	**100**
Channel and Frequency	**92.77**	**91.47**	**8.53**	**0**	**100**	**100**
Encryption Type	**91.11**	**89.07**	**10.92**	**0**	**100**	**100**
Timestamp and Sequence Count	**85.55**	**82.61**	**17.38**	**0**	**100**	**100**

From all the above results it is observed that the highest accuracy of 92.77% is achieved with the use of SSID and MAC spoofing parameters for RAP detection. The highest TPR of 91.81% and lowest FNR of 8.19% is achieved in the same scenario.

The memory utilization before and during the execution of the implemented solution on Ubuntu, Kali, Redhat Linux is shown in the graph of figure 5.17. It is also observed that the primary memory required to run the program is only 16%. This proves that the implemented system has negligible performance overhead in terms of memory utilization.

The comparison of detection times of implemented and existing methods is given in table 5.20 as well as in the graph in figure 5.51.

Table 5.20: Comparison of detection times of implemented and existing method

RAP detection time of existing paper method [5] (milliseconds)	RAP detection time of implemented method (milliseconds)
345	233
797	257
797	278
803	405
685.5	**293.25**

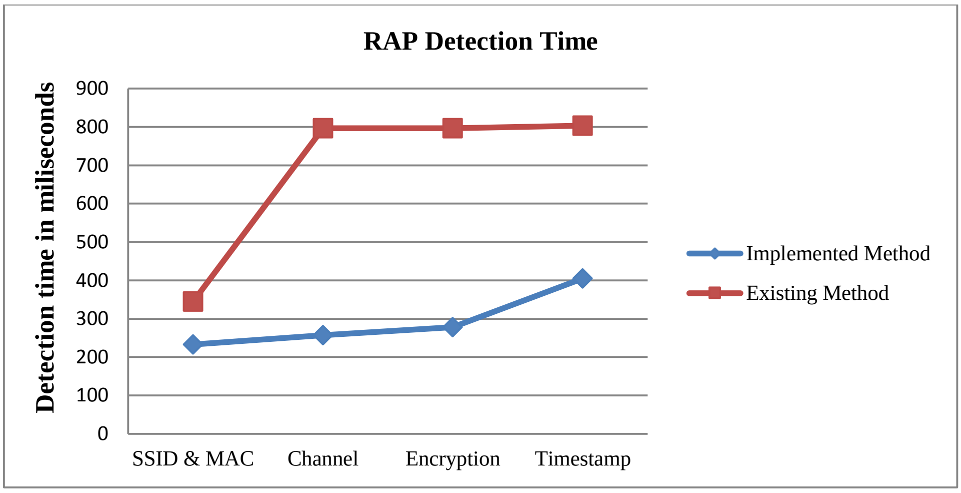


Figure 5.51: Graphical Analysis of RAP Detection Time

From the graph it is observed that the average detection time by implemented method is 293 msec. which indicates approximately 37.33% reduction in detection time as compared to the detection time of 468 msec. required by existing method [1]. Table 5.20 shows the comparison of existing methods and the implemented Multiparameter method. Highest accuracy and minimum detection time is achieved using the Multiparameter method.

Table 5.21 Comparison with Existing Methods

Sr. No.	Evaluation Parameter	E M (5)	E M (21)	E M (11)	E M (1)	E M (23)	Multiparameter Method
1	Accuracy	85%	68%	90%	81.39 %	NA	**92.77%**
2	FPR	8%	NA	12.5 %	6.52%	1%	**0**
3	FNR	8.2 %	NA	16%	NA	NA	**8.19%**
4	Detection Time (msec.)	685.5	907	900	468	985	**293.25**

The implemented solution is installed on only one node unlike other researchers' solution that requires installation on multiple nodes. The beacon frame broadcasted by the AP is used to extract the values of all the parameters like SSID, MAC address, channel, frequency, encryption, RSS value, time-stamp and sequence count. Table 5.21 compares the Multiparameter method with five Existing Methods (EM) from different reference papers.

5.8.2 Understanding Performance Improvements

After using the multi parameter based method, major improvement is observed in both, detection time as well as accuracy. After thoughtful experiments and rigorous analysis, the reasons for these improvements are listed below.

1. Most of the existing methods are based on analysis of network traffic. When this network traffic is analyzed centrally, then the servers need to be computationally

extremely superior. As huge amounts of data packets are analyzed along with their headers and payloads, the time required for successful detection of RAP increases exponentially, degrading the entire system performance. On the other hand, multi parameter based method checks only few parameters in the wireless header. This drastic reduction in comparisons helps in achieving major system performance improvements.

2. Existing methods, which do not use network traffic characteristics, make use of techniques requiring more computational time. For example, distributed computing based methods usually take lot of computational time as they require additional time for intra system data transfer and subsequent algorithm convergence. Hence these methods also show performance degradation.
3. Existing methods that employ artificial intelligence, distributed computing, clock skew, machine learning etc. to detect RAPs use parameters that are dynamic in nature and change drastically with change in network and experimental setup. Therefore it is very difficult for these methods to sustain their accuracy level irrespective of experimental setup. Multi-parameter method uses parameters that are independent of underlying platform or execution environment. This helps in sustaining accuracy under different scenarios.

CHAPTER-6

CONCLUSION

The implemented system combines multiple parameters to detect RAPs in the WLAN. In this implementation, real time data is used for testing of RAP detection tool. Average RAP detection time of this tool is 293 milliseconds with TPR of 91.81%, FNR of 8.19 % and TNR of 100%, FPR of 0% and Precision of 100%. Accuracy of the tool is 92.77% for SSID and MAC address spoofing attack. Thus the accuracy is improved by 2.77% as compared to the method in reference paper [11], and the detection time is improved by 37.33%, as compared to the method in reference paper [1]. It is also observed that the primary memory required to run the program is only 16%.

The evaluation shows effectiveness of the system in detecting MITM attack with negligible performance overhead. The developed multi parameter method has unique features such as,

- Easy deployment,
- Rapid scalability,
- Independent of signal frequency, MAC, traffic type and training data.

The main contribution of this research work is use of two additional parameters viz. sequence count and timestamp for RAP detection.

Existing techniques do not provide an optimum solution. Implemented approach considers all the parameters for RAP detection and provides an optimum solution without modifying network architecture.

6.1 Future Scope

The system can be further modified

- To minimize RAP detection time to a lower value.
- To increase accuracy and minimize false positive rate.
- To develop more robust RAP detection system which can detect more WLAN attacks and prevent them.
- To block the detected RAP.
- To configure the security policies using artificial intelligence.
- To detect presence of rogue vehicles and vehicle tracking.

PUBLICATIONS

International Conference and Journals:

1. S.B.Vanjale, Dr.P.B.Mane, "Detection of Rogue Access Point Using Various Parameters" Paper presented in International conference ICDECT 2016 held on 15th February 2016 and will be published in **Springer Proceedings (AISC)**.
2. S.B.Vanjale, Dr.P.B.Mane, S.V.Patil, "Wireless LAN Intrusion Detection and Prevention System for Malicious Access Point" International Conference on "Computing for Sustainable Global Development, 11th- 13th March 2015 at Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA). INDIACom-2015; ISSN 0973-7529, ISBN 978-93-80544-15-1.Page No. 585 to 591. Print ISBN: 978-9-3805-4416-8/15/$31.00 c 2015 **IEEE**.
3. S.B.Vanjale, Dr.P.B.Mane, "A Novel Approach for Elimination of Rogue Access Point in Wireless Network", 11th IEEE India International Conference Indicon 2014 on "Emerging Trends and Innovation in Technology", 11th - 13th December 2014 at Yashada, Pune, India. Paper No- 373. DOI: 10.1109/INDICON.2014.7030418.INSPEC Accession Number: 14904004, **Print ISBN:** 978-1-4799-5362-2.
4. S.B.Vanjale, Jay Dave, Dr.P.B.Mane, "Unapproved Access Point Avoidance Approach for WLAN: New Algorithm" Proceedings of International Journal of Recent trends in engineering and sciences**,** IJRTES Vol.2, Issue 2, April 2012**.** ISSN: 2277-3258.
5. S.B.Vanjale, Jay Dave, Dr.P.B.Mane, "Unapproved Access Point Elimination in WLAN Using Multiple Agents and Skew Intervals" Proceedings of International Journal of Engineering Science and Technology, IJEST Vol. 4, No.02, February 2012. ISSN: 0975- 5462.
6. Swati Jadhav, S.B.Vanjale, Dr.P.B.Mane, "Illegal Access Point Detection Using Clock Skews Method in Wireless LAN", International Conference on "Computing for Sustainable Global development", 5th- 7th March 2014 at Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM),New Delhi.(INDIA)**.** INDIACom-2014; ISSN 0973-7529, ISBN

978-93-80544-10-6.Page No. 836 to 841. DOI: 10.1109/IndiaCom.2014.6828057. INSPEC Accession Number: 14382798.

7. Amit Chougule, S.B.Vanjale, Dr.P.B.Mane, "Detection and Prevention of Rogue Access Point in the 802.11 using various parameters", in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)/Vol.- 5/ Issue-5/May- 2015.ISSN: 2277-128X.
8. M.K.Nivangune, S.B.Vanjale, Dr.P.B.Mane, "Detecting Unauthorized Access Point in WLAN by using CTT", in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)/Vol.-5/ Issue-7/July-2015. ISSN: 2277-128X.
9. M.K.Nivangune, S.B.Vanjale, Dr.P.B.Mane, "Wireless LAN Intrusion detection by using statistical timing approach" Proceedings of International Journal of Research in Engineering and Technology (IJRET)/Vol.-3/ Issue-11/Nov- 2014. EISSN: 2319-1163 | ISSN: 2321- 7308.
10. S.V.Patil, S.B.Vanjale, Dr.P.B.Mane, "Wireless LAN Intrusion Detection System (WLIDS) For Malicious Access Point", Proceeding of 4th International Conference Organized by IRAJ Research Forum, 13th July 2014, ISBN-978-93-84209-36-0.
11. Swati Jadhav, S.B.Vanjale, Dr.P.B.Mane, "Wireless Rogue Access Point Detection Using Clock Skew Method", Proceedings of International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 3, Issue 10 October 2013 ISSN: 2277 128X.
12. Swati Jadhav, S.B.Vanjale, Dr.P.B.Mane, "On Wireless Rogue Access Point Detection Using Clock Skew Method" Proceedings of International Journal of Advanced Research in Computer Science and software March 2013 (IJARCSS).
13. S.V. Patil, S.B.Vanjale, Dr.P.B.Mane, "A Survey on Malicious Access Point Detection Methods For Wireless Local Area Network" Proceedings of International Journal of Computer Science and Engineering (IJCSE)/Vol.-2/Issue-3/March 2014.E ISSN: 2347-2693.
14. S.Thite, S.B.Vanjale, Dr.P.B.Mane, "A Novel approach for Fake Access point Detection and Prevention in Wireless Network" Proceedings of International Journal of Computer Science Engineering and Information Technology",

(IJCSEITR)/Vol.-4/ Issue-1/Feb 2014. ISSN: 2249-7943(Online) and ISSN: 2249-6831(Print).

15. S.Thite, S.B.Vanjale, Dr.P.B.Mane, "Elimination of Rogue access point in Wireless Network", Proceedings of International Journal of Scientific and Engineering Research"(IJSER) /Vol.-4/ Issue-12/ December-2013.ISSN:2229-5518(Online).
16. M.K.Nivangune, S.B.Vanjale, Dr.P.B.Mane, "A Survey on Unauthorized AP detection in WLAN By Measuring DNS RTT", Proceedings of International Journal of Computer Science and Technology (IJCST)/Vol.-4/Issue-2/April-June 2013.ISSN:0976- 8491(Online) and ISSN: 2229- 4333(Print).
17. Sachin Sonawane, S.B.Vanjale, Dr.P.B.Mane, "A Survey on Evil Twin Detection Methods for Wireless Local Area Network", Proceedings of International Journal of Computer Engineering and Technology (IJCET) /Vol.-4/ Issue-2/March-April 2013.ISSN:0976-6375(Online) and ISSN: 0976-6367(Print).
18. Sachin Sonawane, S.B.Vanjale, Dr.P.B.Mane, "Wireless LAN Intrusion Prevention System (WLIPS) For Evil Twin Access Points", Proceedings of International Journal of Computer Science and Technology (IJCST)/Vol.-4/ Issue-2/April-June 2013.ISSN:0976-8491(Online) and ISSN: 2229-4333 (Print).
19. Fatima Mulla, S.B.Vanjale, Dr.P.B.Mane, "Providing Data Security for Wi-Fi network using mobile agent in distributed system", Proceedings of International Journal of Advanced Engineering Technology**,** IJAET/Vol.3/ Issue II/April-June, 2012**.** E-ISSN 0976-3945.
20. Sushma Shirke, S.B.Vanjale, Dr.P.B.Mane, "On Fast and Accurate Detection of Unauthorized Access Point Using Time Stamp in WLAN", Proceedings of International Journal of Computer Science and Technology, IJCST Vol.2, Issue 3, September 2011, ISSN: 2229-4333(Print)| ISSN: 0976-8491(Online).
21. S.B.Vanjale, Dr.P.B.Mane, "WLAN Intrusion Detection System", Proceedings of International Journal of Computer Science and Management Studies, Volume 11, Issue 02, Aug 2011,IJCSMS, ISSN (Online)2231-5268.
22. Fatima Mulla, S.B.Vanjale, Dr.P.B.Mane, "Illegal Access Point Detection for Wi-Fi Network By Using Hybrid Approach" Proceedings of International

Journal of Advanced Engineering Technology, IJAET, E-ISSN 0976-3945, Volume. II, Issue IV, October-December, 2011.

23. Snehal Behede, S.B.Vanjale, Dr.P.B.Mane, "Detection of Illegal Access Points Using Filters and Network Attacks Using Signatures for Providing Security in WLAN", Proceedings of International Journal of Engineering Research and Indu. Appls. (IJERIA).ISSN 0974-1518, Vol. 4, No.III (August 2011), pp. 309-318.

24. Fatima Mulla, S.B.Vanjale, Dr.P.B.Mane, "Unauthorized Access Point Detection for Wi-Fi Network by Using Hybrid Approach", Proceedings of International Journal of Engineering Research and Industrial Applications.(IJERIA). ISSN 0974-1518, Vol. 4, No. III (August 2011), pp.285-296.

25. Sushma Shirke, S.B.Vanjale, Dr.P.B.Mane, "Rogue Access Point Detection Using Time Stamp" International Journal of advanced Computer and mathematical sciences. ISSN:2230-9624 June 2011 Volume: 02, issue: 02, pp 111-116.

26. Amol Kadam, S.B.Vanjale, Dr.P.B.Mane, "Detecting and Eliminating Rogue Access Point in IEEE 802.11 WLAN" Proceedings of International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) Volume – 1, Issue-1, 2011.

27. Pramod Jadhav, S.B.Vanjale, Dr.P.B.Mane, "Integrated Rogue Access Point Detection System And Counter Attack in Wireless LAN" Proceedings of Journal of Emerging Technologies And Applications In Engineering Technology And Science.(IJ-ETA- ETS).ISSN-0974-3588 January –June 2011. Vol.4, Issue 1, Page No-210-13.

28. Snehal Behede, S.B.Vanjale, Dr.P.B.Mane, "Providing Data Security in WLAN by Detecting Unauthorized Access Points and Attacks" Proceedings of International Journal of Engineering Science and Technology (IJEST). ISSN: 0975-5462, Vol. 3 No.5 May 2011.

REFERENCES

[1] Yang, Chao, Yimin Song, and Guofei Gu, "Active user-side Evil Twin access point detection using statistical techniques." Information Forensics and Security, IEEE Transactions on, Vol. 7, no. 5: 1638-1651, 2012.

[2] K. Kao, I-En Liao, and Y-C Li, "Detecting rogue access points using client-side bottleneck bandwidth analysis", in Proceedings of the Science Direct, computers and security, 2009.

[3] T. Kim, H. Park, H.Jung, and H. Lee, "Online detection of fake access points using received signal strength", in Proceedings of the IEEE 75th International conference on Vehicular Technology, 2012.

[4] L. Ma, A. Y. Teymorian, and X. Cheng, "A hybrid rogue access point protection framework for commodity Wi-Fi network", in Proceedings of the IEEE INFOCOM, 2008.

[5] M. Song G. Shivraj and S. Shetty, "A hidden markov model based approach to detect rogue access points", in Proceedings of the IEEE, 2008.

[6] S. Nikbakhsh, A. Manaf, M. Zamani, and M. Janbeglou, "A novel approach for rogue access point detection on the client side", in Proceedings of the International conference on Advanced Information Networking and Applications workshops, 2012.

[7] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews", in Proceedings of the 14th ACM international conference on Mobile computing and networking (MobiCom), 2008.

[8] T. Kindberg, J. Mitchell, C. Bevan, and ONeill, "Authenticating public wireless network with physical evidence", in Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and communication, 2009.

[9] Bo Yan, Guanling Chen, JieWang, Hongda Yin "Robust Detection of Unauthorized Wireless Access Points", Published online: 1 November 2008 © Springer Science.

[10] Roth, V., Polak, W., Rieffel, E. and Turner, T., (2008). "Simple and effective defense against Evil Twin Access Points", WiSec'08, March 31–April 2, 2008, Alexandria, Virginia, USA.

[11] H. Han, B. Sheng, C. Tan, Q. Li, and S. Lu., "A timing based scheme for rogue AP detection", in Proceedings of the IEEE Transactions on parallel and distributed systems, 2011.

[12] Srilasak, S. Wongthavarawat, K. Phonphoem, A, "Integrated Wireless Rogue Access Point Detection and Counterattack System"**,** Information Security and Assurance, IEEE CNF April 24-28, 2008, Pathumthani, Thailand.

[13] Shetty, Sachin, Song, Min ,Ma, Liran, "Rogue Access Point Detection by Analyzing Network Traffic Characteristics", Military Communications Conference, 2007. MILCOM 2007, IEEE, Orlando, FL, USA.

[14] Raheem Beyah, Shantanu Kangude, George Yu, Brian Strickland, and John Copeland, "Rogue Access Point Detection using Temporal Traffic Characteristics," *in Proceedings of IEEE GLOBECOM*, Dec. 2004.

[15] Han, H., Lu, Lu, X.L., and Ren, L.Y., "Using Data Mining to Discover Signatures in Network-Based intrusion detection", in Proceeding of IEEE Computer Graphics and Applications,2002, pp.212-217.

[16] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill. "Enhancing the security of corporate Wi-Fi networks using DAIR", in Proceeding ACM MOBISYS, 2006, Uppsala, Sweden.

[17] H. Yin, G. Chen, and J. Wang., "Detecting Protected Layer-3 Rogue APs", in Proceedings of the Fourth IEEE International Conference on Broadband Communications, Network, and Systems",(BROADNETS),Raleigh, NC, September 2007, Raleigh, NC, USA.

[18] Lanier Watkins**,** Raheem Beyah**,** Cherita Corbett, "A Passive Approach to Rogue Access Point Detection" IEEE Communications Society, IEEE GLOBECOM 2007 proceedings,1930-529X/07/$25.00 © 2007 IEEE.

[19] M. Tung, Le1, Ren Ping Liu2, and Mark Hedley "Rogue Access Point Detection and Localization" published in IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC) sept.2012. INSPEC Accession Number**:** 13167039, 2012.

[20] V. S. Shankar Sriram, G. Sahoo, Krishna Kant Agrawal, “Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology”, published in Advance Computing Conference (IACC), 2010 IEEE 2nd International, INSPEC Accession Number:11155873. Feb 2010.

[21] Wei Wei, Kyoungwon Suh, Bing Wang, “Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK- Pairs”, IMC’07, IEEE CNF, San Diego, California, USA, October 24-26, 2007.

[22] Beyah, R.; Venkataraman, A., "Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions", IEEE Security and Privacy, vol.9, no.5, pp.56, 61, Sept.-Oct. 2011.

[23] J. Yang, Y. Chen, W. Trappe, J. Cheng “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks” in IEEE Transactions on Parallel and Distributed Computing (Volume: 24 , Issue: 1) DOI- 10.1109 TPDS.2012.104. Jan 2013.

[24] Sia Sie Tung, Nurul Nadia Ahmad, Tan Kim Geok,“Wireless LAN Security: Securing Your Access Point” IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006.

[25] Donald R. Reising, Member, IEEE, Michael A. Temple, Senior Member, IEEE, and Julie A. Jackson, “Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints” ,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 6, JUNE 2015.

[26] Thambo Nyathi, Siqabukile Ndlovu, “Beacon Frame Manipulation to Mitigate Rogue Access Points: Case of Android Smartphone Rogue Access Points”, COMPUSOFT, An international journal of advanced computer technology, 3 (2), February-2014 (Volume-III, Issue-II).

[27] Hao Han, Fengyuan Xu, Chiu C. Tan, Yifan Zhang, Qun Li, “Defending Against Vehicular Rogue Aps”, IEEE Infocom 2011.

[28] Jonny Milliken, Valerio Selis and Alan Marshall, “Detection and analysis of the Chameleon WiFi access point virus” Milliken et al. EURASIP Journal on Information Security 2013 a SpringerOpen Journal.

[29] Sartid Vongpradhip, Wichet Plaimart, "Survival Architecture for Distributed Intrusion Detection System (DIDS) using Mobile Agent" Sixth IEEE International Symposium on Network Computing and Applications (NCA 2007) 0-7695-2922-4/07 $25.00 © 2007.

[30] Hao Han, Bo Sheng, Chiu C. Tan, "A Measurement Based Rogue AP Detection Scheme" 978-1-4244-3513-5/09/$25.00 ©2009 IEEE.

[31] Gaogang XIE , Tingting HE , Guangxing ZHANG "Rogue Access Point detection Using Segmental TCP Jitter" WWW 2008 / Poster Paper April 21-25, 2008 Beijing, China

Web Sites

[32] www.airdefense.net.

[33] www.airmagnet.net.

[34] www.netstumbler.com.

[35] www.kismetwireless.net.

[36] www.airsnort.shmoo.com

[37] www.airsnare.com.

[38] www.airjack.soft112.com

[39] www.aircrack-ng.org

[40] www.airtightnetworks.net.

[41] www.kaspersky.com

Books

[42] Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill.

[43] Stewart S. Miller, "Wi-Fi Security", McGraw-Hill.

[44] Charles B. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", Third Edition,

[45] William Stallings, "Cryptography and Network Security – Principles and Practices", Pearson Education, Third Edition.