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.
Chapter 1: Introduction

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 smartphones 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:

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration/ID</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Sequence Control</th>
<th>Address 4</th>
<th>Frame Body</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>0-2312</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC HEADER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragment Number</td>
</tr>
</tbody>
</table>

**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.
Chapter 1: Introduction

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(4,6),(993,991)
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.

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.