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.

![Diagram of the system](image.png)

**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>
<thead>
<tr>
<th>Parameter</th>
<th>Existing System</th>
<th>Implemented System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distance</td>
<td>150 ft.</td>
<td>In between 150 to 300 ft.</td>
</tr>
<tr>
<td>Network Latency</td>
<td>Marginal</td>
<td>Negligible</td>
</tr>
<tr>
<td>RAP Detection Time</td>
<td>1 Min</td>
<td>Less than 1 Min</td>
</tr>
</tbody>
</table>

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](image)

### 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

![Image of Intrusion Detection System]

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.

![LEARNING MODE Diagram]

**LEARNING MODE**

- **Packet Handler Module**
- **Packet Extractor**
- **List Builder**
- **File Module**
- **Checker**

![DETECTION MODE Diagram]

**DETECTION MODE**

- **Packet Handler Module**
- **Packet Extractor**
- **List Builder**
- **File Module**
- **Checker**
- **RSSI Verifier**
- **Detector**
- **Disassociation**

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 lists, the network administrator easily identify authorized and unauthorized access points 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>
<thead>
<tr>
<th>Sr. No.</th>
<th>SSID</th>
<th>MAC Address</th>
<th>RSSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Android AP</td>
<td>00:02:6f:5f:39:a3</td>
<td>-94</td>
</tr>
<tr>
<td>2</td>
<td>SST</td>
<td>20:10:7a:39:db:39</td>
<td>-78</td>
</tr>
<tr>
<td>3</td>
<td>BVCOEW</td>
<td>f8:1a:67:a1:06:cd</td>
<td>-93</td>
</tr>
<tr>
<td>4</td>
<td>Nano-con</td>
<td>bc:79:ad:52:81:ae</td>
<td>-40</td>
</tr>
<tr>
<td>5</td>
<td>IDEA-GPRS</td>
<td>00:7a:39:db:39:f8</td>
<td>-39</td>
</tr>
<tr>
<td>6</td>
<td>BVOCEP</td>
<td>52:81:5f:39:06:cd</td>
<td>-52</td>
</tr>
<tr>
<td>7</td>
<td>BVG</td>
<td>06:cd:ad:52:6f:5f</td>
<td>-49</td>
</tr>
</tbody>
</table>

3.3.5.2 Detection Mode

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

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.

![System Execution Sequence](image)

**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 skews of AP with that of the existing one to display whether AP is Fake or authorized.
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>
<thead>
<tr>
<th>Number of Packets Examined</th>
<th>Estimation of Clock Skews</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Skew (using LSF)</td>
</tr>
<tr>
<td>100</td>
<td>19.74 ppm</td>
</tr>
<tr>
<td>200</td>
<td>34.71 ppm</td>
</tr>
<tr>
<td>300</td>
<td>51.86 ppm</td>
</tr>
<tr>
<td>400</td>
<td>26.86 ppm</td>
</tr>
</tbody>
</table>

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

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 a 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, a hybrid framework is designed. This framework can forecast 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.

![Diagram of Distributed Monitoring 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 differentiate the authorised and unauthorized AP. By observing the OS fingerprints it checks 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 checks for unregistered MAC and duplicate MAC.
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](image1)

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](image2)

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.

![Diagram of RAP detection using multiple agents and skew intervals](image)

**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.
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.