Wireless Pers Commun (2018) 98:139–156
https://doi.org/10.1007/s11277-017-4860-5

Multi Parameter Based Robust and Efficient Rogue AP Detection Approach

Sandeep B. Vanjale[1] · **Pradeep B. Mane**[2]

Published online: 22 August 2017

Abstract Wireless LANs are an integral part of todays 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. Existing 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. From the results it is observed that the developed multi-parameter based method shows improvement in terms of time required for detecting RAP. Detection time is improved by 37.33%, in comparison to the different methods.

Keywords Rogue access point · WLAN security · RAP detection · IEEE 802.11

✉ Sandeep B. Vanjale
sbvanjale@bvucoep.edu.in

Pradeep B. Mane
pbmane6829@rediffmail.com

[1] Computer Engineering Department, Bharati Vidyapeeth Deemed University, College of Engineering, Pune, Maharashtra 411043, India

[2] Department of Electronics Engineering, AISSMS's IOIT, Pune, Maharashtra, India

1 Introduction

The increase in the number of smartphone users in the world has been impressive. Now a days, 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. 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. According to a report insufficient information regarding secured wireless network, can cause various threats on security.

2 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 authorize 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].

2.1 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.

An attacker can configure network deployment to implement Man-In-The-Middle (MITM) attack on any client. The 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 clients connection will be changed. This connection can later be used for stealing important information.

Even if firewall is present in a network, it can not detect RAP. 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 Wi-Fi Protected Access version 2 (WPA2) 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 security control cannot be enforced on it. RAP threats work at a layer below wired IDS and antivirus [2].

2.2 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 analyses the data traffic in real time. Due to antenna, range of AP wireless transmission is limited to certain distance.

2.3 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 [3].

2.4 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.

2.5 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 [4].

2.6 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 [5].

2.7 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.

2.8 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.

2.8.1 Vulnerabilities of WPA2

Although WPA 2 is improved version it still has plenty of vulnerabilities. Some existing vulnerabilities of WPA2 [6] are discussed below.

- 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 de-authenticate, 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.

3 Limitations of Existing Methods

Limitations of existing RAP detection methods are:

1. ***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.
2. ***Inter Packet Arrival Time***—Can be used to detect RAPs, but it is not effective when Evil Twin is present [7].

3. ***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 [8].
4. ***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 [9].
5. ***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 [10].
6. ***Wireless Traffic***—In wireless environment, network traffic can provide inaccurate results. Such inaccurate results create a suitable environment for RAP to perform attacks [11].
7. ***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 [12].

4 Design of the Multi-parameter RAP Detection Method

4.1 Factors Affecting RAP Detection Techniques

- ***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***—Existing techniques use wireless traffic between client and access point for detection of RAP. In wireless environment, 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

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

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. 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). Every channel has a unique frequency range from 2412 to 2484 MHz with a difference of 5 MHz each.

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 Flowchart

Figure 1 shows the flowchart of the implemented approach:

4.4 Mathematical Model

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

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

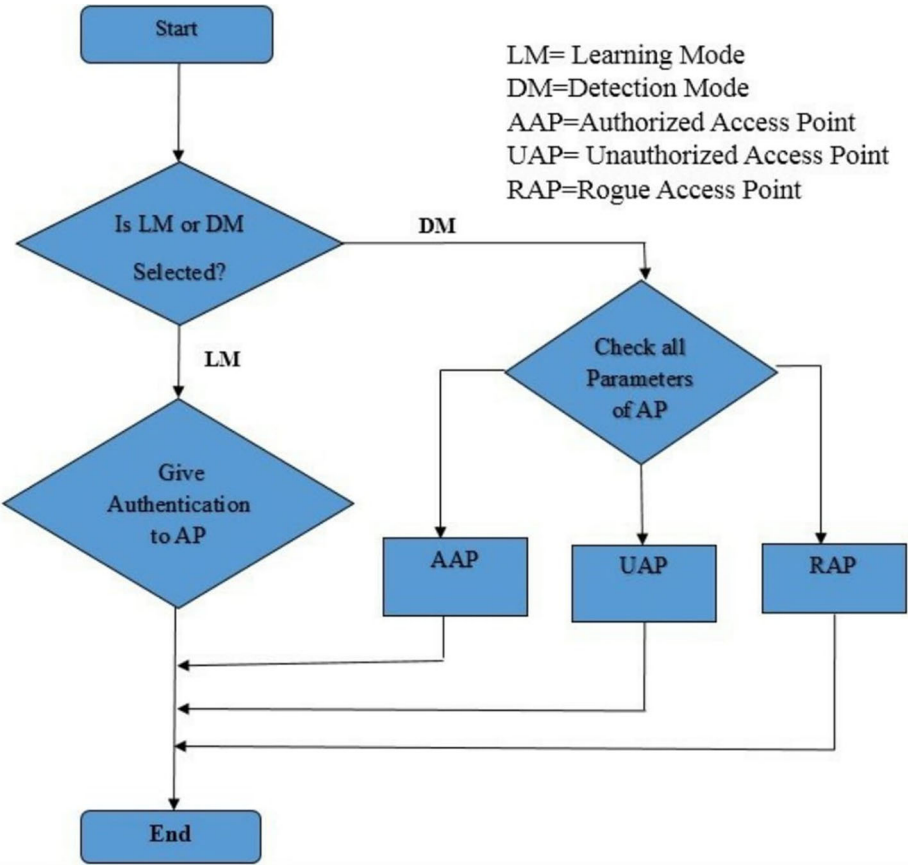

Fig. 1 Flowchart of RAP detection method

Table 1 Parameter description

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

Each access point contains different parameters as given in Table 1.

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,

$$B \backslash A = \{x \in B | x \notin A\} \tag{1}$$

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

Hence,

$$D_L \backslash W_L = \{x \in D_L | x \notin W_L\} \tag{2}$$

Using Eq. 2, RAPs can be inferred by the implemented system, if result set of Eq. 2 is a not an empty set ($\neg \varnothing$).

4.5 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 B_{ssid} with W_{ssid}
If not matched then add to rogue AP list and go to Step 1
Step 4: CompareB_{mac} with W_{mac}
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: CompareB_{ts} with W_{ts}
If not matched, then add to rogue AP list and go to Step 1
End

5 Architecture

Figure 2 shows the system architecture of the implemented approach:

5.1 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,

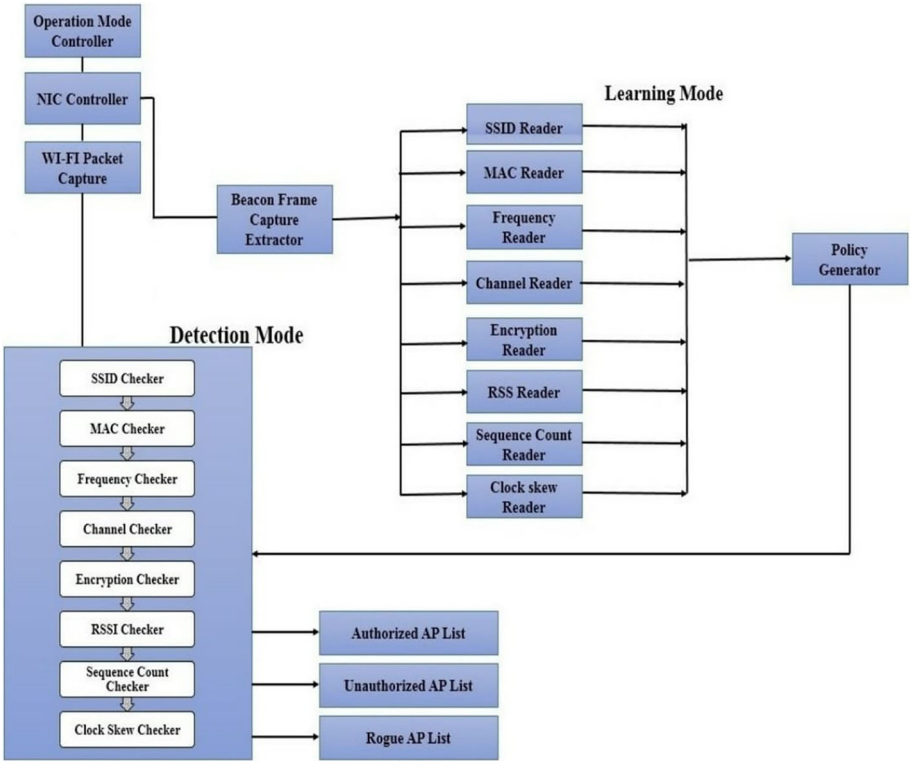

Fig. 2 System architecture of implemented approach

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.

5.2 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.

6 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. 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.

7 Evaluation

7.1 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 2. One RAP was inserted to test effectiveness of software in detection mode using received signal strength of wireless access point as shown in Table 3. The RAP was configured using same SSID and channel as that of an authorized access point in the network. 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.

Table 2 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 3 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

- ***Scenario 2-Evil Twin Attack*** Figure 3 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.
- ***Scenario 3-MAC address spoofing attack*** Figure 4 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

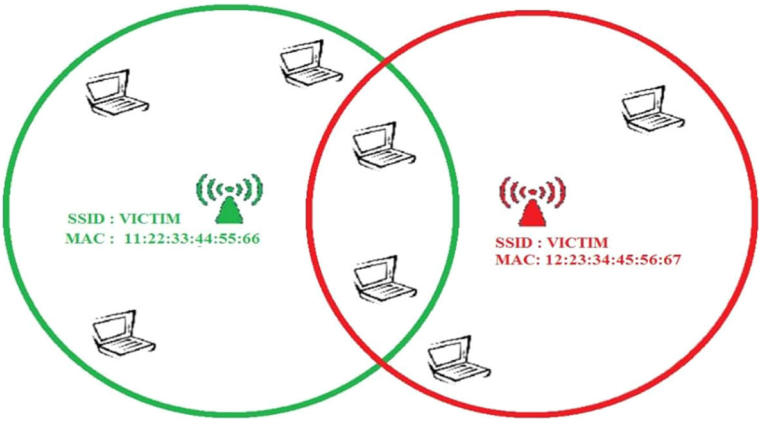

Fig. 3 Evil twin with same SSID

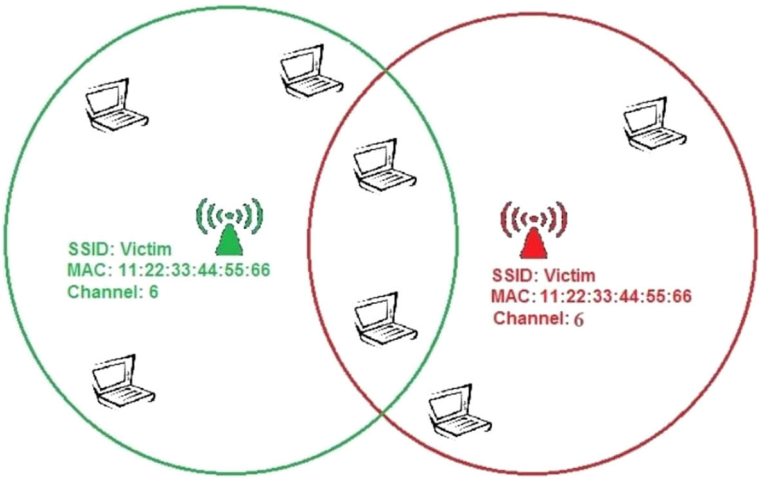

Fig. 4 SSID and MAC address spoofing attack

in the right side of the figure in red color. The authorized access points in the networks are shown in Table 4. 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. 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.

The legitimate access point uses encryption to connect to the network. But the RAP does not use encryption as shown in Table 5. 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.

7.2 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

Table 4 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 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

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 byL_{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.

7.3 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 Fig. 5.

7.4 Detection Time

To test the environmental effect on the detection time of implemented system, tests were performed for a period of 1 week during morning, afternoon and evening time slots. Total

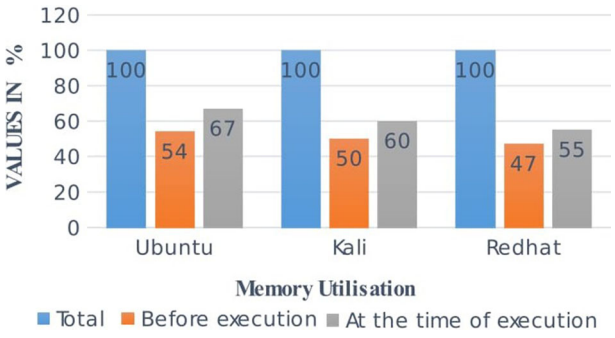

Fig. 5 Memory utilization during execution of implemented system

Table 6 Detection time for 7 days three times in a day

Day	Morning detection time (ms)	Afternoon detection time (ms)	Evening detection time (ms)
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
Avg. detection time (ms)	0.427667344	0.43856222	0.499522763

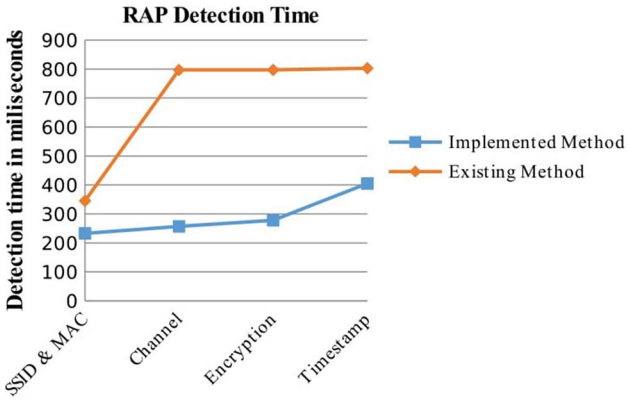

Fig. 6 Graphical analysis of RAP detection time

Table 7 Comparison of detection times of implemented and existing method

RAP detection time of existing method (ms)	RAP detection time of implemented method (ms)
345	233
797	257
797	278
803	405
685.5	293.25

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.

Table 6 provides detection time at three different times in a day for a period of 1 week, which indicates that there is a slight variation in the detection time of RAP.The comparison

of detection times of implemented and existing methods is given in Table 6 as well as in the graph in Fig. 6.

8 Conclusion and Future Scope

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 ms. The detection time is improved by 37.33%, as compared to other methods given in Table 7. It is also observed that the primary memory required to run the program is only 16%. The system detects MITM attack with negligible performance overhead. The developed multi parameter method has unique features are 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. Implemented approach considers all the parameters for RAP detection and provides an optimum solution without modifying network architecture.

The system can be further modified to minimize RAP detection time to a lower value, increase accuracy and minimize false positive rate. It can be used for the development of more robust RAP detection system which can detect more WLAN attacks and prevent them, or block the detected RAP. Further, it can be used with artificial intelligence to detect presence of rogue vehicles and vehicle tracking.

References

1. Han, H., Xu, F., Tan, C. C., Zhang, Y., & Li, Q. (2011). Defending aganist vechicluar rogue Aps. In *IEEE Infocom 2011*.
2. Nikbakhsh, S., Manaf, A., Zamani, M., & Janbeglou, M. (2012). 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*.
3. Milliken, J., Selis, V., & Marshall, A. (2013). Detection and analysis of the Chameleon WiFi access point virus. *EURASIP Journal on Information Security 2013 a Springer Open Journal*, *2013*, 2.
4. Le, T. M., Liu, R. P., & Rogue, M. H. (2012). Access point detection and localization published in IEEE 23rd international symposium on personal, indoor and mobile radio communications-(PIMRC). INSPEC Accession Number: 13167039.
5. Reising, D. R., Temple, M. A., & Jackson, J. A. (2015). Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints. *IEEE Transactions on Information Forensics and Security*, *10*(6), 1180.
6. Beyah, R., & Venkataraman, A. (2011). Rogue-access-point detection: Challenges, solutions, and future directions. *IEEE Security and Privacy*, *9*(5), 5661.
7. Han, H., Sheng, B., Tan, C., Li, Q., & Lu, S. (2011). A timing based scheme for rogue AP detection. In *Proceedings of the IEEE transactions on parallel and distributed systems*.
8. Nyathi, T., & Ndlovu, S. (2014). 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), 576.
9. Yang, J., Chen, Y., Trappe, W., & Cheng, J. (2013). Detection and localization of multiple spoofing attackers in wireless networks. *IEEE Transactions on Parallel and Distributed Computing*. doi:10.1109/TPDS.2012.104.
10. Kim, T., Park, H., Jung, H., & Lee, H. (2012). Online detection of fake access points using received signal strength. In *Proceedings of the IEEE 75th international conference on vehicular technology*.

11. Yang, C., Song, Y., & Guofei, G. (2012). Active user-side Evil Twin access point detection using statistical techniques. *IEEE Transactions on Information Forensics and Security*, *7*(5), 1638–1651.
12. Shankar Sriram, V. S., Sahoo, G., Agrawal, & Krishna K. (2010). Detecting and eliminating rogue access points in IEEE-802.11 WLAN: A multi-agent sourcing methodology. In: *2010 IEEE 2nd international published in advance computing conference (IACC)*. INSPEC Accession Number: 11155873.

Sandeep B. Vanjale is working as a Professor in Computer Engineering Department at Bharati Vidyapeeth University College of Engineering, Pune, Maharashtra, India. He received his M.E. (Computer) and Ph.D. degrees from Bharati Vidyapeeth University College of Engineering, Pune. His research interests include Computer Network, Network Security, WLAN Security. He attended more than 40 National and International Conferences and published 50 papers in International Conference and Journals.

Pradeep B. Mane received his B.E. (E&Tc) and M.E. (E&Tc) degree from Government College of Engineering Pune, India and Ph.D. from Bharati Vidyapith University. He worked in Philips India ltd. for 3 years, 15 years in Bharati Vidyapeeth University COE Pune and currently working as a principal in AISSMSs Institute of Information Technology, Pune. He was a member of the BOS for Electronics faculty in Bharati Vidyapeeth University. He has co-authored five books for engineering courses with Technova publications pune in the subjects of Radio and TV engineering and computer networks. He has published 40 papers in National, International Conferences and seminars. He has 15 National and International Journal publications. He is a regular reviewer for Springer Wireless Communications Journal. His area of interest is Wireless Communication and Networking. He is a fellow of IETE and ISTE.