Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection and Prevention of Rogue Access Point in the 802.11 Using Various Parameters

Amit A. Chougule
MTech Scholer
Department of Computer, Engineering, BVUCOE, Pune, India

Prof. Sandip B. Vanjale
Ph.D.Research Scholar
Department of Computer Engineering, BVUCOE, Pune, India

Dr. P. B. Mane
Ph.D.Research Guide, BVU Pune
Professor, Department of Electronics Engineering, AISSSMS,s IOIT Pune, India

Abstract - Now a day's wireless network has gained immense popularity due to low cost and easy installation. Today we can use 802.11 for many purposes for example sharing data, for social media, publish personal blogs etc. the popularity of 802.11x WLAN inherently causes dangerous situation in respect of the security of the data of the user. One of such risky situations is in concern with the network security specifically wireless security regarding rogue wireless access point. A RAP is not validly authorised by any company or organisation for its operation. A RAP unnecessarily intervenes in the data of the sensitive network. This paper tries to provide solution to the problem of RAP in the wireless network in respect of their security risk and also tries to give valid authorization and make them secure using various parameters.

Keywords: 802.11, Rogue AP, Authorized AP, network Security.

I. INTRODUCTION

At present the people use various devices to communicate or interact with each other. This devices can be divided into two segments wired device and wireless device. In the First Segment Wired Devices the communication or interaction depends upon the wires. Whereas in the second segment wireless device is no need of any external thing like wire. Notwithstanding the fact, some or other Access point has to be used for communication. Access Point is an agent which acts as a medium between wired and wireless devices. An access point is divided in two categories. One is authorized access point and other one will be unauthorized access point. Authorized Access point can be stated to be one which has been validly authorized to operate unauthorized Access point can be neighbours which has not been authorized at all to operate. Unauthorized Access point can be classified into two sub sections the first being rogue access point where as the second is fake access point.

It can said that the people may turn to the unauthorized access point because of there lake of knowledge or literacy. Regarding the wireless network security it may cause irreparable harm to data of the user. It necessitates the efforts minimising the harm to the user and the loss of the confidence of the wireless network security.

This paper deals with the problem of wireless network security specifically regarding rogue access point with usage of various access point parameter therefore section II describes various wireless Access Parameter. Section III reviews the historical perspective consideration. Section IV will highlight the proposed system with results. Section V will conclude this paper.

II. WIRELESS ACCESS POINT PARAMETER

1. SSID:

SSID is a term used in short form for Service Set Identifier. SSID comprises 32 characters. There can be multiple SSID's in the network never the less each one of them plays unique role in its own way. The function of SSIDs is to regulate the process which makes sure that the data is reaches to its desired destination.

There can be Multiple Access Points having the same SSID In single network. It is impossible to communicate the data without SSID.

2. MAC Address:

MAC is a term used in short from for media access control. Physical network segment is communicated by MAC Address which is assigned to network interfaces. It is also a unique identifier.

The usage of MAC is done in human-friendly form comprising 48 bits in six octets. Each of them contains two hexadecimal digits partitioned by colons (:) or hyphens (-). Out of six, the first three octets give the information about organisation exquisitely. Next three are used for identifying Network Interface Card (NIC).

3. RSSI:

RSSI is a term used in short from for Received Signal Strength Indicator. The quality of communication between the sensor unit and the Access point is indicated by the RSSI value and it is expressed as Decibels (dB). The

RSSI values are appears in a negative number because of low power levels and free air attenuation.

Table No. 1 RSSI values Range with their quality

RSSI Range	Signal Quality
Better than -40 dB	Exceptional
-40 dB to -55 dB	Very Good
-55 dB to -70 db	Good
-70 dB to -80 dB	Marginal
-80 dB and beyond	Intermittent to No Operation

RSSI values can vary from 0 to -100. The value showing nearness to 0 signifies strong signal whereas the value approaching -100 indicates weaker signal.

4. Channel and Frequency:

Wireless channels are used to transmit the information signals from one or more senders to one or more receivers. The transmitting capacity of the channel is measured in bandwidth in Hz or its data rate in bits per second.

Wireless Network consist 13 channels which are unlicensed. Each channel has its own unique frequency from 2412 MHz to 2484 MHz with difference of 5MHz.

Table No. 2 Channels with their Frequency

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

5. Authentication type:

Every user wants to have authenticated and secured communication with the other and the policy providing this facility to the users is called authentication. Authentication is divided into three types namely

a. WEP

WEP is a term used in short from for Wired Equivalent Policy. WEP is a older method of security used in case of older devices which is easy to hack. Therefor it is not recommended presently.

b. WPA

WPA is a term used in short from for Wi-Fi Protected Access. WPA provides guaranty to the user that only authorized people should have access to it. WPA is sub divided in two parts first one is WPA and other is WPA2.

c. 802.1X Authentication

It enhances security for 802.11 wireless network. It provides network access with validity.

6. Radio Type:

There are several standards prepared by IEEE for wireless network with a suffix letter. It covers every standard including security aspects and quality service.

Table No. 3 standards of 802.11x

Standard name	802.11a	802.11b	802.11g	802.11n
Standardization date	January 2000	December 1999	June 2003	June 2009
Maximum bandwidth	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Modulation technique	OFDM	DSSS, CCK	DSSS, CCK, OFDM	DSSS, CCK, OFDM+
RF band	5 GHz	2.4 GHz	2.4 GHz	2.4 or 5 GHz
Channel bandwidth	20 MHz	20 MHz	20 MHz	20 or 40 MHz

7. First Time Seen:

When a particular Access Point is detected a specific time will be displayed that is called first time seen. When detection process is repeated then each access point's detection time will change. But after authorization with the process of authentication the first time seen time of the authorised access point will never change and the time will be the when that access point has become authorised.

8. Last Time Seen:

Like the first time seen the last time seen will not remain the same. It will keep on changing unlike the first time seen.

III. RELATED WORK

Hemanshu Kamboj and Gurpreet Singh have proposed Detection of Fake Access Point to Prevent Session Hijacking. In this paper they have given a solution for the problem of session hijacking and also suggested measures for the prevention of session hijacking. Session hijacking is a one of the most troublesome active attack. They have used RSSI value as a parameter to detect fake access points.

Ms. Swati Jadhav, Prof. S.B.Vanjale and Prof.Dr. P.B.Mane have proposed Illegal Access Point Detection Using Clock Skews Method in Wireless LAN. They have used timestamp and the sequence count as a parameter to detect illegal access points.clock skew is the differance between two consecutive timestamps.

Mr. Sandip Thite, Prof. Sandeep Vanjale and Prof. P. B. Mane have proposed a system on Elimination of Rogue access point in Wireless Network. In this system they have used RSSI value, MAC address and the channels for detecting rogue access points. They have used Aircrack-ng Software freely available on the internet to detection of Access points.

Thambo Nyathi and Siqabukile Nd lovu have proposed the Beacon Frame Manipulation to Mitigate Rogue Access Points: Case of Android Smartphone Rogue Access Points.

IV. PROPOSED SYSTEM

In this module we broadcast request to access point. Available Access point Give response for that request. In this module we get header information is in a response. Headers have raw information .Then we extract the packet in readable format. After that we have details properties of access point .now we have list of all access point. We create white list.

White list contains details about Access point. We give White list as input for Detection Module.

After process of Authentication we detect unauthorized access point and also rouge access point in wireless Network. In this module we get input from learning module which is white list .we scan access point periodically we check properties of access point & white list access point. We use SSID, MAC Address, Authentication type, Channel, Frequency, and Signal for detection.

if SSID is Same then we check Mac Address is same then we check Authentication type is same then we check channel etc. properties of access point if some properties are match then we assign access point is rouge access point. Process is given bellow,

1. Start Application
2. Log in Application
3. Activate Wi-Fi Scanner
4. Get header Information of Scan Wi-Fi access point
5. Extract Packet information from header information
6. Get list of Access point with details (properties)
7. Detect Rouge access point from list of access point.
8. Provide White list for Detection.
9. Gives the output.
10. Stop Application

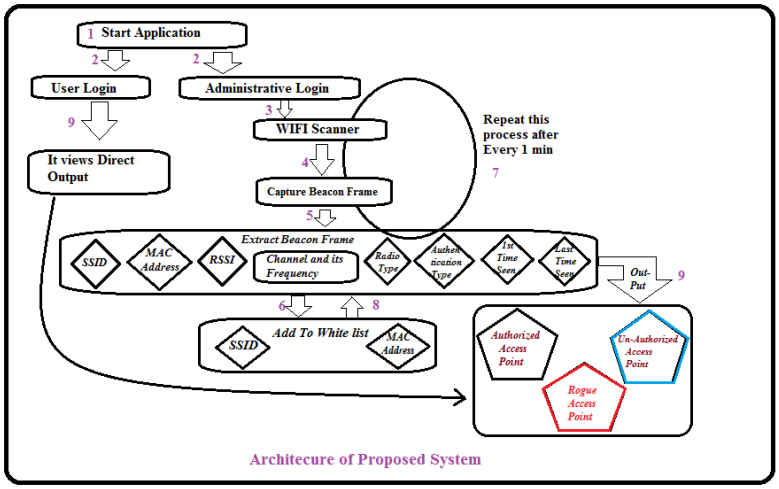
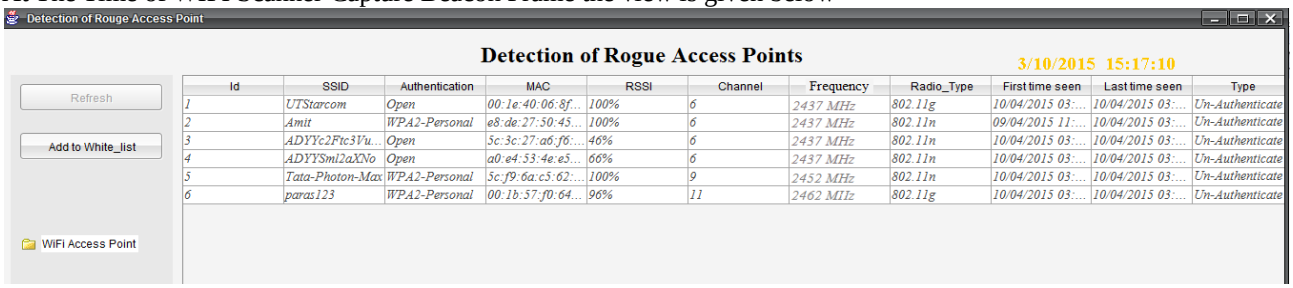


Fig. 1 Architecture of Proposed System

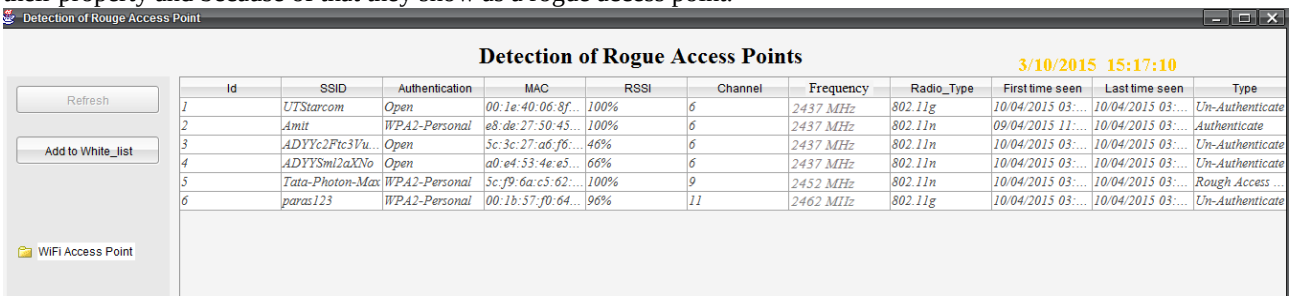
V. RESULTS

At The Time of WIFI Scanner Capture Beacon Frame the view is given below



Id	SSID	Authentication	MAC	RSSI	Channel	Frequency	Radio_Type	First time seen	Last time seen	Type
1	UTStarcom	Open	00:1e:40:06:8f...	100%	6	2437 MHz	802.11g	10/04/2015 03:...	10/04/2015 03:...	Un-Authenticate
2	Amit	WPA2-Personal	e8:de:27:50:45...	100%	6	2437 MHz	802.11n	09/04/2015 11:...	10/04/2015 03:...	Un-Authenticate
3	ADYYc2Ftc3Vu...	Open	5c:3c:27:a6:f6:...	46%	6	2437 MHz	802.11n	10/04/2015 03:...	10/04/2015 03:...	Un-Authenticate
4	ADYYSml2aXNo	Open	a0:e4:53:4e:e5...	66%	6	2437 MHz	802.11n	10/04/2015 03:...	10/04/2015 03:...	Un-Authenticate
5	Tata-Photon-Max	WPA2-Personal	5c:f9:6a:c5:62:...	100%	9	2452 MHz	802.11n	10/04/2015 03:...	10/04/2015 03:...	Un-Authenticate
6	paras123	WPA2-Personal	00:1b:57:f0:64...	96%	11	2462 MHz	802.11g	10/04/2015 03:...	10/04/2015 03:...	Un-Authenticate

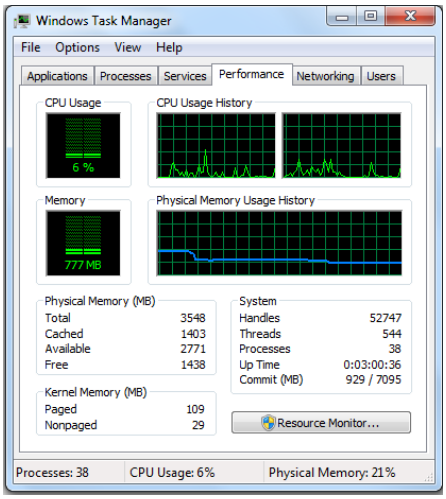
After giving Authorization to Access Points the result gets as they are authorized or Unauthorized or they have changed their property and because of that they show as a rogue access point.



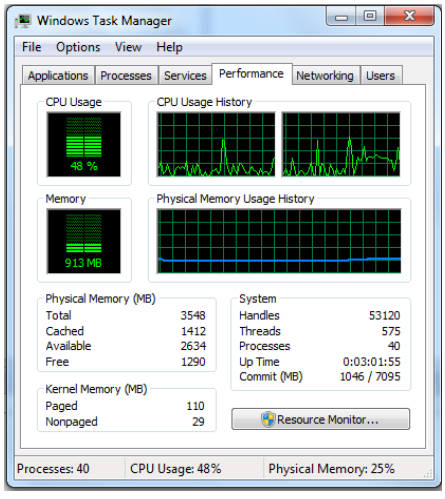
Id	SSID	Authentication	MAC	RSSI	Channel	Frequency	Radio_Type	First time seen	Last time seen	Type
1	UTStarcom	Open	00:1e:40:06:8f...	100%	6	2437 MHz	802.11g	10/04/2015 03:...	10/04/2015 03:...	Un-Authenticate
2	Amit	WPA2-Personal	e8:de:27:50:45...	100%	6	2437 MHz	802.11n	09/04/2015 11:...	10/04/2015 03:...	Authenticate
3	ADYYc2Ftc3Vu...	Open	5c:3c:27:a6:f6:...	46%	6	2437 MHz	802.11n	10/04/2015 03:...	10/04/2015 03:...	Un-Authenticate
4	ADYYSml2aXNo	Open	a0:e4:53:4e:e5...	66%	6	2437 MHz	802.11n	10/04/2015 03:...	10/04/2015 03:...	Un-Authenticate
5	Tata-Photon-Max	WPA2-Personal	5c:f9:6a:c5:62:...	100%	9	2452 MHz	802.11n	10/04/2015 03:...	10/04/2015 03:...	Rough Access ...
6	paras123	WPA2-Personal	00:1b:57:f0:64...	96%	11	2462 MHz	802.11g	10/04/2015 03:...	10/04/2015 03:...	Un-Authenticate

Performance of System:

Before Executing Application



After Executing Application



V. CONCLUSIONS

In this research i have worked on the detection of rogue access points in the network and then prevent the user from rogue access points. To prevent i have used various parameters like ssid, mac address, rssi value, etc.

REFERENCES

Websites:

[1] Airdefense enterprise: WIPS. Available: http://www.airdefense.net.
[2] Airmagnet. Available: http://www.airmagnet.com.
[3] AirTight Network. Available: http://www.airtightnetwork.com.
[4] Netstumbler. Available: http://www.netstumbler.com.

Journals:

[1] Patil, S., & Vanjale, S. (2014). A Survey on Malicious Access Point Detection Methods for Wireless Local Area Network. *International Journal of Computer Sciences and Engineering*, *2*, 22-25.
[2] Shourbaji, I. A., & AlAmeer, R. (2013). Wireless Intrusion Detection Systems (WIDS). *arXiv preprint arXiv:1302.6274*.
[3] Scahill, F. J., & Evenden, R. J. (2014). *U.S. Patent No. 20,140,325,615*. Washington, DC: U.S. Patent and Trademark Office.
[4] Halasz, D. E., & Andrade, M. B. (2007). *U.S. Patent No. 7,181,530*. Washington, DC: U.S. Patent and Trademark Office.
[5] Zhang, Y., & Lee, W. (2000, August). Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 275-283). ACM.
[6] Thite, M. S., Vanjale, S., & Mane, P. B. Elimination of Rogue access point in Wireless Network. International Journal of Scientific & Engineering Research, Volume 4, Issue 12, November-2013 ISSN 2229-5518.
[7] Paper published on topic "A Novel approach for Fake Access point Detection and Prevention in Wireless Network" in International Journal of Computer Science Engineering and Information Technology"(IJCSEITR)/Vol.-4/ Issue-1/Feb 2014.ISSN:2249-7943(Online) and ISSN:2249-6831(Print).
[8] Paper published on topic "A Survey On Malicious Access Point Detection Methods For Wireless Local Area Network " in International Journal of Computer Science and Engineering (IJCSE)/Vol.-2/Issue-3/March 2014.E ISSN:2347-2693.
[9] Paper published on topic "On Wireless Rogue Access Point Detection Using Clock Skew Method " in International Journal of Advanced Research in Computer Science and software March 2013 (IJARCSS).
[10] Paper published on topic "Wireless Rogue Access Point Detection Using Clock Skew Method " in International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE). Volume 3,Issue 10 October 2013 ISSN: 2277 128X .
[11] Paper published on topic "Wireless LAN Intrusion Detection System (WLIDS) For Malicious Access Point " in Proceeding of 4th International Conference Organized by IRAJ Research Forum on 13 th July 2014. ISBN-978-93-84209-36-0.
[12] Paper published on topic "Wireless LAN Intrusion detection by using statistical timing approach " in International Journal of Research in Engineering and Technology"(IJRET)/Vol.-3/ Issue-11/Nov- 2014. eISSN: 2319-1163 | pISSN: 2321-7308.

