Wireless LAN Intrusion Detection and Prevention System for Malicious Access Point with Live Attacks

Prof. Poonam Rajput[1], Prof. Sandip V. Patil[2], Prof. Chhayadevi H. Khambalkar[3]

[1]Ph.D. Research Scholar, Department of Information Technology, BVIOT, Navi Mumbai, India.
[2] Ph.D. Research Scholar, Department of Forensic, KPMG, Pune, India
[3]Ph.D. Research Scholar, Department of Computer Engineering, BVCOE, Pune, India.

---***---

Abstract - In latest trends, Wireless Access Points are popularly used for the convenience of smart mobile users. The growing popularity of Wireless Local Network (WLAN) put forth different dangers of wireless security attacks. A Malicious Access Point might be set in any open spaces so as to imitate honest to goodness Access Points for adaptation. Existing malicious Access Point detection methods analyze wireless traffic by using extra devices, and the data of traffic is collected by servers. Malicious Access Points, if undetected, can take important information from the network. Numerous attackers took advantages of the undetected Malicious Access Points in ventures to not just get free Internet Access, and yet to view classified informative content. The vast majority of the present results for identify Malicious Access Points are not automated. In this research paper, we consider the problem of "malicious" attacks in wireless local area networks (WLANs). A Malicious is essentially a rogue (phishing) Wi-Fi access point (AP) that looks like a legitimate one (with the same SSID) and we consider an unprotected client, other networks client to avoid wireless unauthorized clients not only the detect and prevent but we show and enlist the live attackers details.

Keywords – WLAN, MAP, DOS, MITMA, Evil Twin, FIN, SYN Attack.

1. INTRODUCTION

WLAN Security technology has major use in many fields. Wireless LAN has a wide range of applications due to its flexibility and easy access. The use of public Wi-Fi has reached at a level that is difficult to avoid. While users (especially smart phone users) can access Wi-Fi wireless internet "hotspot" connections in public more easily, they become to be more vulnerable to fraud and identity theft, referred to as Malicious attacks. Malicious is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers. The main things are what many papers in only client side or server side is protecting not all systems. So our solutions are automatically detects malicious access points on the network and block them and protect to unprotected clients also. And most novelty points in our system to protect to unauthorized client and also protect other networks unauthorized clients. We have created the white list in that containing authorized clients. And compare their IP Address, SSID, Detection/Prevention Time and MAC Address then find out the unauthorized AP or clients.

Our main contributions are as follows:

1. We examined and analyzed different types of techniques to detect and prevent Malicious Access Points.

2. We implement a new lightweight server and client side malicious detection and prevention solution.

3. We implement efficiently to detect and prevent Malicious Access Points on the network.

4. We protect unprotected clients with same network and other networks.

5. We detect and prevent live attacks. Like FIN, SYN.

6. We use the four factor IP Address, SSID, Detection / Prevention TIME and MAC Address.

2. BACKGROUND

Various security mechanisms are necessary in order to avoid threats against Wireless Local Networks. Different threats are exist on the Wireless Network; one of such serious threat is Malicious Access Point. A Malicious attack is quick and easy to set as shown in fig. 1, attacker can easily set Malicious access point and looks like the authorized access point used in public Wi-Fi area, these area could be coffee shop, restaurants, airport...etc. Attacker can set up malicious access point near to the victims, the malicious access point then try to attack the victim's wireless connection by using different methods and force victim to change the connection. Generally Malicious AP uses powerful wireless signals then the authorized AP inside the range. User's laptop or other devices automatically get connected to the AP with highest RSSI. Once victim is connected to the Malicious AP, by catching network packets between Malicious AP and the authorize AP the attacker can provide internet access and can get sensitive information similar to passwords, credit and debit card details...Etc. In this way Malicious AP works as a "Malicious" AP between victim and the authorize AP. the attacker can bring out more serious attacks like phishing. In short, malicious attack is a dangerous threat to the WLAN Security.

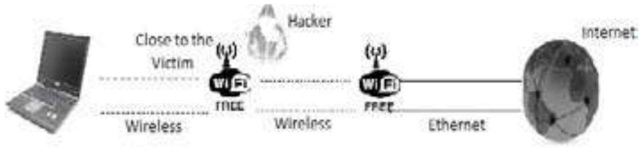


Fig. 1: Malicious Attack

3. RELATED WORK

The threat of Malicious AP has attracted both industrial and academic researchers to focus on this problem. There are some methods presented which deal with this problem. Hao Han and his colleagues used timing based scheme for Malicious AP detection [1], in that they have functional timing based plan for the client to avoid from connecting with Malicious AP. In their discovery system they have utilized timing informative content dependent upon the round trek time. Thought is to client test a server in neighborhood and after that measure the RTT from the reaction, this methodology is rehashed number of times and all RTTs are recorded. Provided that the mean worth of RTTs is bigger than a fixed threshold, they acknowledge the partnered AP as a Malicious AP. They have acknowledge four elements that have impact on timing RTT which are Data transmission rate, Location of DNS server, Wireless movement and APs workload. They have tried precision of their method recognizing distinctive situations for these four components.

Taebeom Kim and his colleagues utilized received signal strengths for discovery of Malicious Access Point [2], in this they measures corresponded RSS arrangements from adjacent APs keeping in mind the end goal to figure out if the sequences are honest or fake. This system works in three stages. In stage one they are gathering RSS from adjacent AP. In Second Phase they are doing standardization of gathered RSSs, it assesses some missed RSSs, caused by some outside variables and standardizes the evaluated RSSs for generalization of an assortment of wireless environments. In third stage they are figuring out which RSSs are greatly corresponded to others dependent upon some empirical threshold value. They outline that remarkably associated RSS sequences as fake signals from a single device.

Qu and Nefcy presented new indirect Malicious Access Point detection system [3] they broke down local round trip time (LRTT) information and composed a system with numerous calculations for identifying wireless hosts effectively. Their work begins from inactively examining or observing system movement to have disclosure and catching Client-side solution for Malicious Access Point.

Assuming that customer is associated with remote server through Malicious AP and a standard AP that is two-hop remote channel, so this gives the thought to discover Malicious attacks by differentiating one-hop and two-hop remote channels from the client to the remote server. In this they have utilized two calculations, first is Trained Mean Matching, in this they are utilizing preparing method to distinguish Malicious attack. The second calculation is Hop Differentiating Technique; it is a non-preparing-based location calculation in which they are utilizing specific speculative worth for the limit to distinguish malicious attack. They have tried this strategy under diverse RSSI levels for the correctness of the recognition of Malicious AP.

TABLE I. Comparison of various Papers

Paper Topic	Author Name	Year of Publics	Weakness	Algo.
Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point	Yimin Song, Chao Yang, and Guofei Gu	2010 IEEE	wireless infrastructures (e.g., 3G or WiMax)	Trained Mean Matching (TMM) and Hop Differentiating Technique (HDT).
Active User-side Evil Twin Access Point Detection Using Statistical Techniques	Chao Yang, Yimin Song, and Guofei Gu, *Member, IEEE*	2011 IEEE	Distance, Packet, Hop	Trained Mean Matching (TMM) and Hop Differentiating Technique (HDT).
A Novel Approach for Rogue Access Point Detection on the Client-Side	Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou	2012 IEEE	Only Client Side	Wireless IDS
Online Detection of Fake Access Points using Received Signal Strengths	Taebeom Kim, Haemin Park, Hyunchul Jung, and	2012 IEEE	Distance	Classification of received signal strength

	Heejo Lee			
Elimination of Rogue access point in Wireless Network	Mr. Sandip Thite,	Dec 2013	Distances	RSS
Wireless LAN Intrusion Detection and Prevention System for Malicious Access Point	Prof. Sandip Patil	March 2015 IEEE.	SSID ,IP, MACID, etc	Authentication and De-Authentication rules

4. OUR ANALYSIS

A. Design

In this section we will explain our problem statement and approach. Our solution will work on any type of network that is wired network, wireless network or heterogeneous network. Implemented solutions for client side only. But our solution works for client and server side. So our solution is automatically detects malicious access points on the network and prevent them.

B. Features of the Solution

- Accurate Detection of Malicious AP.
- Less time to detect Malicious AP (2 to 3 ms).
- Scalable Solution.
- Consume very less bandwidth of the network.
- Apart from Detection of Malicious AP, to protect the unprotected clients also.
- Detect and Prevent live attacks. Like FIN, SYN.
- We use the four factor IP Address, SSID, Detection / Prevention TIME and MAC Address.

C. System Architecture

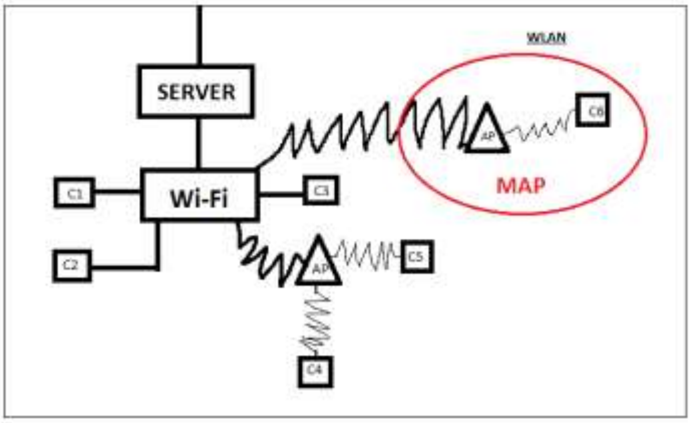


Fig. 2: System Architecture

C1, C2, C3 Wired Device, C4, C5, C6 Wireless Devices, AP: Access Point, MAP: Malicious AP, WLAN wireless network. System Architecture in that we consider the wired network C1 to C3 are wired client and one is the wireless client C4, C5, C6. They are connected to authorize access point like AP, and other things WLAN also create malicious access point like MAP. So they trying to connect authorized client system and connect successfully. And with our system that detect the malicious access point and prevent De-Authentication rule and avoid that client.

D. Implementation.

We have implemented our approach using Python development Kit. We have created the white list in that authorized clients. And compare their IP Address, SSID and MAC Address then find out the unauthorized clients. We evaluated the prototype of our approach on a computer with an Intel Core 2 Duo 2.58GHz CPU and 4GB RAM, running Linux, Windows 7.We have used Three Access Points.

E. Algorithm

```
Input   : Beacon Frames, Provide the authorized AP lists

Output:  IP, SSID, Detection/Prevention Time and MAC address of Malicious AP

Begin

        Scan for beacon frames-Extract SSID & AP's MAC from it;

        Check captured info with white list it match then go to steps 6;

        If doesn't match with white list info then – Malicious AP detected;

        If step 3 is true then invoke prevention;

        Send De-Authorized to Malicious AP;

        Go to step 1

Do nothing;

        Display message Malicious AP is not present;

End
```

Using set theory,

Let,

W_A = White list of APs where {a0, a1… an}

W_D = Detected APs List {d0, d1…dn}

W_M = Malicious AP detected list.

$W_M = W_D - WA$

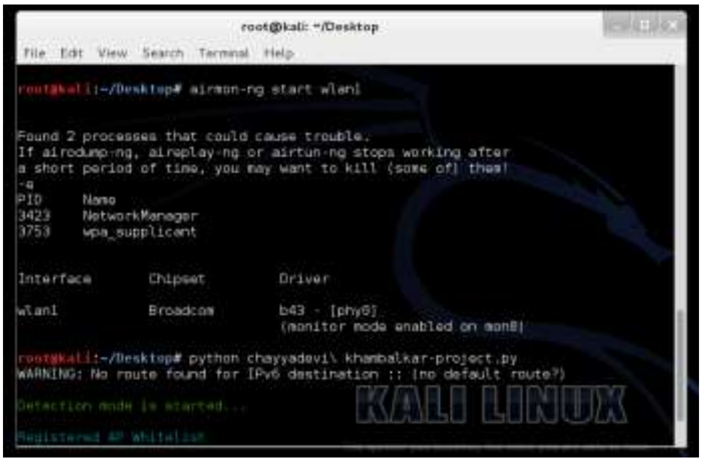
We used Authentication and De-Authentication rules and create the one white list (W_A) in that our authorized client IP, SSID, Detection/Prevention Time and MAC address is store. Only they can access the wireless network. W_D is detected access point list, and W_M is malicious access point detected list. As per set theory we get an unauthorized client lists.

F. Results of Our Solution

This software is being tested with 2 Access Points with 1 Access Point as malicious Access Point and 1 Access Points as authorized Access Points.

```
root@kali:~# cd Desktop/
root@kali:~/Desktop# 
```

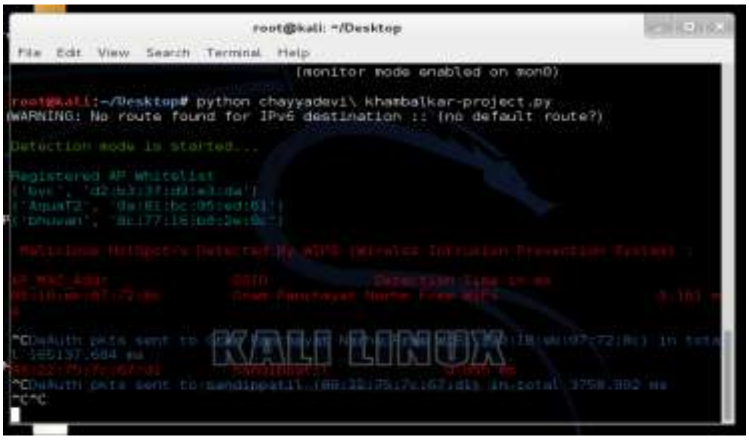
Fig. 3: Detection



```
root@kali:~/Desktop# airmon-ng start wlan1


Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
3423    NetworkManager
3753    wpa_supplicant


Interface       Chipset         Driver

wlan1           Broadcom        b43 - [phy0]
                                (monitor mode enabled on mon0)

root@kali:~/Desktop# python chayyadevi\ khambalkar-project.py
WARNING: No route found for IPv6 destination :: (no default route?)

Detection mode is started...

Registered AP Whitelist
```

Fig. 4: Interface

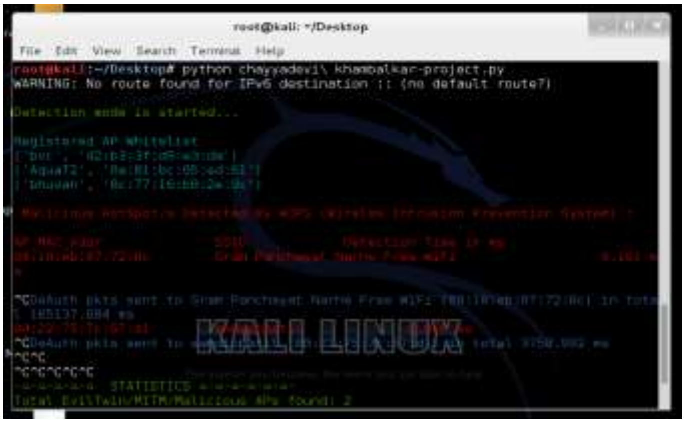
Interface in that to enable the interface card by some command.



```
                    (monitor mode enabled on mon0)

root@kali:~/Desktop# python chayyadevi\ khambalkar-project.py
WARNING: No route found for IPv6 destination :: (no default route?)

Detection mode is started...

Registered AP Whitelist
('bvk', 'd2:b3:3f:d9:e3:da')
('AquaT2', '9a:81:bc:05:ed:61')
('bhuvan', '8c:77:16:b8:2e:9c')

 Malicious HotSpot/s Detected By WIPS (Wireless Intrusion Prevention System) :

AP MAC Addr          SSID                             Detection Time in ms
88:18:ae:87:72:8c    Gram Panchayat Nashe Free WiFi                   0.161 m
s

^CDeAuth pkts sent to Gram Panchayat Nashe Free WiFi (88:18:ae:87:72:8c) in tota
l 165137.684 ms
88:22:75:7c:67:d1    sandippatil              0.066 ms
^CDeAuth pkts sent to sandippatil (88:22:75:7c:67:d1) in total 3758.992 ms
^C^C
```

Fig. 5: Whitelist

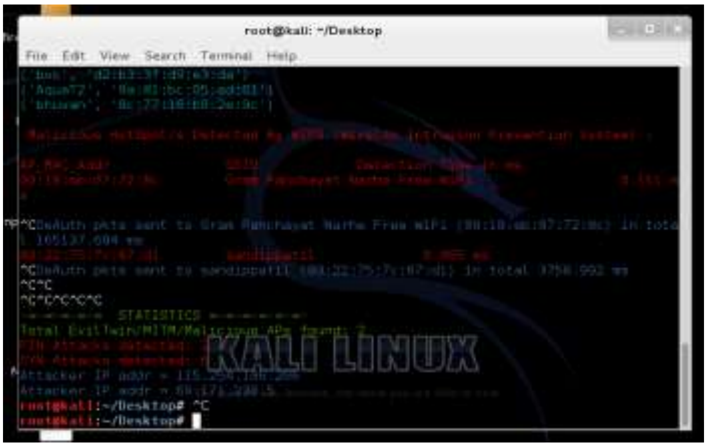
Detection in that to run our system and detection mode is start. So they will show white list or authorized AP and unauthorized AP.



```
root@kali:~/Desktop# python chayyadevi\ khambalkar-project.py
WARNING: No route found for IPv6 destination :: (no default route?)

Detection mode is started...

Registered AP Whitelist
('bvk', 'd2:b3:3f:d9:e3:da')
('AquaT2', '9a:81:bc:05:ed:61')
('bhuvan', '8c:77:16:b8:2e:9c')

 Malicious HotSpot/s Detected By WIPS (Wireless Intrusion Prevention System) :

AP MAC Addr          SSID                             Detection Time in ms
88:18:ae:87:72:8c    Gram Panchayat Nashe Free WiFi                   0.161 m
s

^CDeAuth pkts sent to Gram Panchayat Nashe Free WiFi (88:18:ae:87:72:8c) in tota
l 165137.684 ms
88:22:75:7c:67:d1    [illegible]
^CDeAuth pkts sent to [illegible] in total 3758.992 ms
^C^C
^C^C^C^C^C
-=-=-=-=-=  STATISTICS =-=-=-=-=-
Total EvilTwin/MITM/Malicious APs found: 2
```

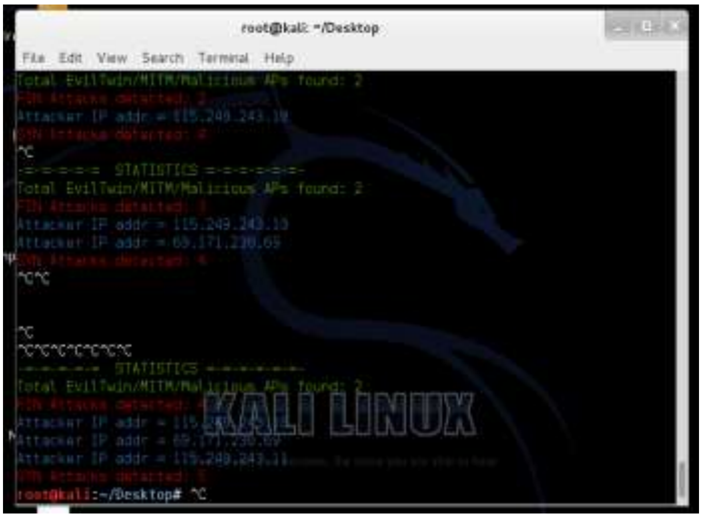
Fig. 6: Detection/Prevention Time

Preventions in that show the malicious access point with IP Address, SSID, Detection/Prevention Time and MAC Address and detection time in milliseconds.



```
('bvk', 'd2:b3:3f:d9:e3:da')
('AquaT2', '9a:81:bc:05:ed:61')
('bhuvan', '8c:77:16:b8:2e:9c')

 Malicious HotSpot/s Detected By WIPS (Wireless Intrusion Prevention System) :

AP MAC Addr          SSID                             Detection Time in ms
88:18:ae:87:72:8c    Gram Panchayat Nashe Free WiFi                   0.161 m
s

^CDeAuth pkts sent to Gram Panchayat Nashe Free WiFi (88:18:ae:87:72:8c) in tota
l 165137.684 ms
88:22:75:7c:67:d1    sandippatil              0.066 ms
^CDeAuth pkts sent to sandippatil (88:22:75:7c:67:d1) in total 3758.992 ms
^C^C
^C^C^C^C^C
-=-=-=-=-=  STATISTICS =-=-=-=-=-
Total EvilTwin/MITM/Malicious APs found: 2
FIN Attacks detected: [illegible]
SYN Attacks detected: [illegible]
Attacker IP addr = 115.254.156.208
Attacker IP addr = 59.171.230.5
root@kali:~/Desktop# ^C
root@kali:~/Desktop# 
```

Fig. 7: FIN/SYN Attacks1



```
Total EvilTwin/MITM/Malicious APs found: 2
FIN Attacks detected: 2
Attacker IP addr = 115.249.243.10
SYN Attacks detected: 4
^C
-=-=-=-= STATISTICS =-=-=-=-=-
Total EvilTwin/MITM/Malicious APs found: 2
FIN Attacks detected: 3
Attacker IP addr = 115.249.243.10
Attacker IP addr = 69.171.230.65
SYN Attacks detected: 4
^C^C


^C
^C^C^C^C^C^C^C^C
-=-=-=-= STATISTICS =-=-=-=-=-
Total EvilTwin/MITM/Malicious APs found: 2
FIN Attacks detected: 4
Attacker IP addr = 115.2
Attacker IP addr = 69.171.230.69
Attacker IP addr = 115.249.243.11
SYN Attacks detected: 5
root@kali:~/Desktop# ^C
```

Fig. 8: FIN/SYN Attacks2

TABLE II. Different Types of Attacks

Sr.No	Attack Type	Live Attack
01	DOS	FIN/SYN
02	MITMA	FIN/SYN
03	Evil Twin	FIN/SYN

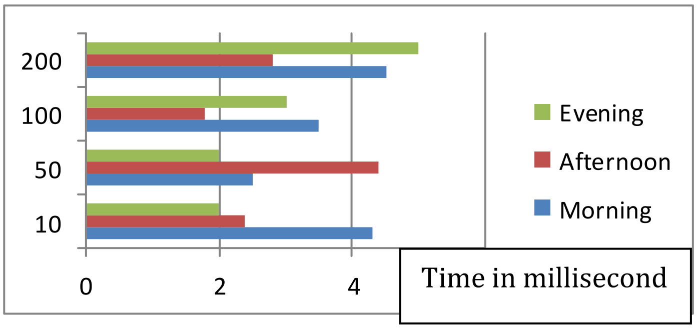


Fig. 9: AP Detection Overhead.

In above graph to access point detect the overhead in various timing. For example Morning, Afternoon and Evening.

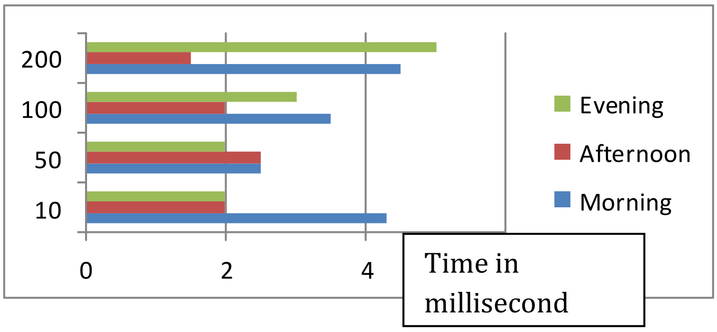


Fig. 10: AP Prevention Overhead.

In above graph to access point prevent the overhead in various timing. For example Morning, Afternoon and Evening.

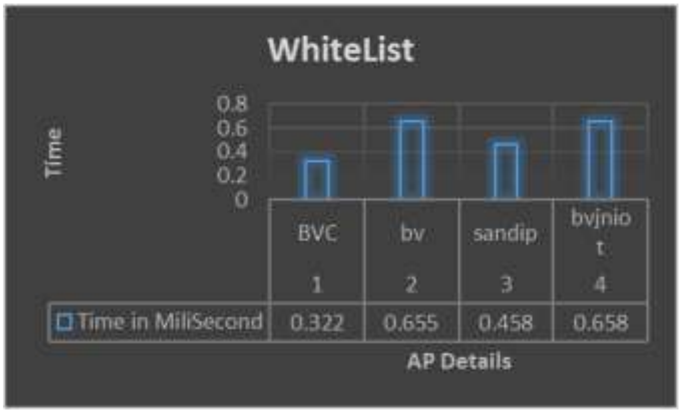


Fig. 11: Whitelists Access Points.

In above graph to authorized access points in particular Network.

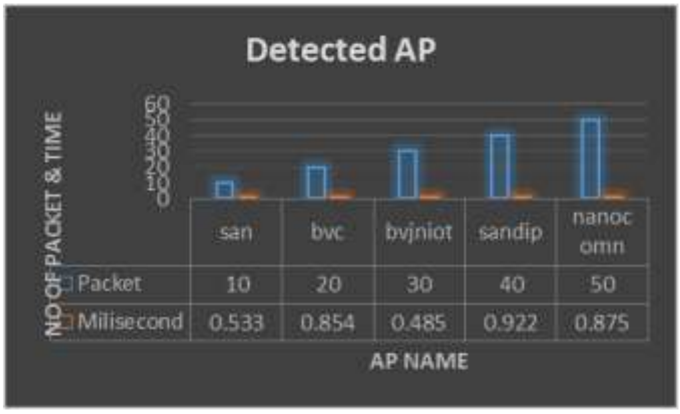


Fig. 12: Detected Access Points.

In above graph to scan in current environment and detect authorized and unauthorized access points.

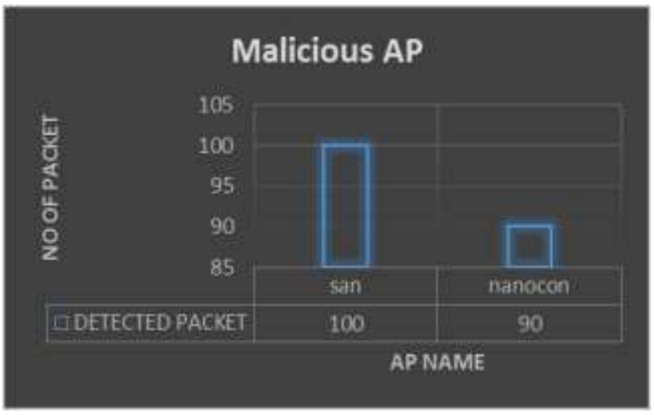


Fig. 13: Malicious Access Points.

In above graph to detect and prevent unauthorized access point by using Authentication and De-Authentication algorithm.

G. Blocking Mechanism

It is important to block Malicious Access Points detected on network. To achieve this, we used Authentication and De-Authentication rules and create the one white list in that our authorized client IP, SSID, Detection/Prevention Time, MAC address are stored. Only they can access the wireless network. Otherwise out of white list IP detected they are not connected because of De-Authentication scenario. Then show the IP, SSID, Detection/Prevention Time and MAC Address as result and also show the detection time.

H. Effectiveness

To measure the effectiveness of our approach, we injected Malicious Access Points in our wireless network. We run our software on server / client; we checked IP Address, SSID, Detection/Prevention Time and MAC Address of devices from captured reply packets and verified them with our authorized AP Point white list database. Our approach successfully detected the Malicious Access Point on our Test scenario.

5. CONCLUSION

We have presented the Intrusion Detection and Prevention Approach for Malicious Access Points in Wireless LAN and live attacks. This technique will work on client side or server side network that is wired network, wireless network.

REFERENCES

1) Hao Han, Bo Sheng, Chiu C. Tan, Qun Li, Sanglu Lu, "A Timing-Based Scheme for Rogue AP Detection", 2011.

2) Taebeom Kim, Haemin Park, Hyunchul Jung, Heejo Lee,"Online Detection of Fake Access Points using Received Signal Strengths", 2012.

3) Chao Yang, Yimin Song, Guofei Gu,"Active User-side Evil Twin Access Point Detection Using Statistical Techniques", 2011.

4) Sandip Patil, “A Survey on Malicious Access Point Detection Methods for Wireless Local Area Network”, IJCSE (E-ISSN: 2347-2693) Vol.2, Issue 3, March 2014.

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

6) Sandeep Vanjale, Dr. P.B.Mane “Detecting and Eliminating Rogue Access Point in IEEE 802.11 WLAN” in Journal of Engineering Research and Studies E-ISSN0976-7916. JERS / Vol.II / Issue III / July-September, 2011.

7) Airdefense enterprise: WIPS. Available: http://www.airdefense.net.

8) Airmagnet.: http://www.airmagnet.com.

9) AirTight Network. Available: http://www.airtightnetwork.com.

10) Aircrack. http://www.aircrack-ng.org.

11) Sandip Patil, “Wireless LAN Intrusion Detection System (WLIDS) for Malicious Access Point”, Goa Conference IRAJ, and 13 July 2014.

12) Sandip Patil, “Wireless LAN Intrusion Detection System (WLIDS) for Malicious Access Point”, Proceedings of 02nd ITR International Conference, 07th September-2014, Bhubaneswar, ISBN: 978-93-84209-50-6

13) Sandip Patil, “Wireless LAN Intrusion Detection and Prevention System for Malicious Access Point”, IndiaCom Conference, Delhi, March 2015.

14) Sandip Patil , “Survey on Detection of Fake Access Point in WLAN”, International Journal of Advanced Research in Computer Science and Software Engineering ,July – 2016.

BIOGRAPHIES

Rajput Punam Udaysing. M.E. Computer Science and Engineering of Aditya Engineering College, Beed under Dr Babasaheb Ambedkar University Aurangabad. She had completed graduation in bachelor of engineering in Computer Science Engineering from Dr Babasaheb Ambedkar University Aurangabad.

Sandip Vasantrao Patil, M.Tech Computer, BVDUCOE,Pune, Maharashtra, India. Research Scholar. Computer Science and Engineering of Bharati Vidyapeeth Deemed University,Pune. He had completed graduation in bachelor of engineering in Computer Science Engineering from Shivaji University,Kolhapur, Maharashtra, India in 2008

Prof.Chhayadevi H. Khambalkar, Phd Student of Department of Computer Engineering, BVCOE, Pune, India