Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detecting Unauthorized Access Point in WLAN by using CTT

[1]M. K. Nivangune, [2]Prof. S. B. Vanjale, [3]Dr. P. B. Mane
[1]M.Tech. Computer Engg, student, BVDUCOE, Pune, India
[2]Ph.D. Research Scholar, Computer Engg,, BVDUCOE Pune, India
[3]Ph.D. Research Guide, BVU, Pune, Professor, Department of Electronics Engg., AISSMS's IOIT, Pune, India

Abstract— Now days the use of accessing internet through Wired or Wireless Local Area Network, has been growing rapidly among the people and In case of Wireless LAN accessing data and information is becoming difficult and the threat of illegal access point (AP) is increasing a lot day by day every day. There are so many different kinds of access points and all of them are completely dedicated to masquerade and attract people to get connect with them. So that internet can be accessed in an illegal/unauthorized way. Here we are finding the solution by experimenting the timing based scheme to stop people from getting connect with illegal access point.

Keywords— WLAN, AP, LAN

I. INTRODUCTION

The Wireless Local Area Networks are completely different than the wired Networks, the wired networks are more secure or we can say physically got more security than the wireless. The data and the information travelling through the air, here anybody can send or receive information and data at any time, the signals or packets doesn't have any security through wires. So that the Wireless Local Area Networks (WLAN) are more vulnerable to the intruders attack. Where anyone can easily break into the network or intercept in between the network in an illegal way, and can have more threat to the system.

The wireless networks are covered by 802.11 standard. The Institute of Electrical and Electronics Engineers (IEEE) have brought this distinction where these people create different standards, and they number these standards in distinct ways. Initially The goals of 802.11 standard are written as follows:-

1) Accessibility
2) Connection

In an another words, the 'open' standard has been developed by 802.11. In early days when security is not at all a major issue, the solutions to the security are really less than the optimal. There are currently a lot of worries about wireless security. Physical connection makes important role in case of Standard networks which are at home or may be at work. If we talk about wireless local area network we don't have any earthly connection. Wireless access points simply makes use of radio transmitters. The use of radio waves takes place in wireless networks which can travel through any obstacle like mountains, buildings, walls etc.. so because of no any earthly connection intrusion is more easy than the wired network. Here we are trying to detect one of the major security concern in case of wireless local area network, i.e. detection of illegal access point.

Two different fake access points can be executed with different devices. The firstly it is wireless router that is used to connect to the Ethernet card directly on the wall. Secondly the fake access points executed on laptop that contains more than two Ethernet wireless cards, one connected to a legitimate access point and another executed as an access point to have access to Internet in WLAN. We will explain the actual difference between above two types of fake access point later, but currently we are working on the second type of fake access point.

Let the internal card or adapter connect to the real access points and the card which is outside is masquerading i.e. pretending to be genuine access point to masquerade users. Now as per standards, when more than one access points are present nearby, a wireless local area network will always select the access point which is having highest signal strength to connect with, so that the fake access point must be close to the clients. The fake access points simply waits for client to connect in passive way but if for more time no client is connected then the fake access points can intentionally send a duplicate frame to make user to change the way.

II. RELATED WORK

The fear of unauthorized access point is increasing fast in WLAN to deal with the problem let's look at some methods Raheem Beyah and Aravind Venkataraman proposed more fundamental wired-side approach to find illegal AP, that has been installed in functionality of MAC based protocol for 802.11 standard. To get the all details of traffic flowing through the wireless networks they simply focusing on the features of two layers of MAC.

Wei Wei, Kyoungwon Suh, Bing Wang, Yu Gu, Jim Kurose, and Don Towsley found a technique that may not be having above drawbacks as it is completely based on passive calculation at particular location, it also posses good scalability only some efforts and cost require for launch, and this is the way by which the design can be easy to handle.

We are aware that here detection is done in WLAN, it is useful to detect fake access points for layer 2 and 3. Whereas the initial approach takes different method for detection of fake access points at various layers. The challenging task for detection of fake access point in second method is wireless detection of traffic from passively gathered data?

Sachin Shetty with Min Song and Liran Ma suggested design approach to detect fake access point. This approach is a solution which can be executed on any router devices in network. The actual reason behind this method is to differentiate legal access point from or station from illegal access point or station by studying different properties in the network. Simulating the results are used to check the efficiency of our method in detection of fake access points in a wireless network consist of both wireless as well as wired networks. The Liran, Min and sachin has implemented the detection of fake access point depends on traffic at distinct network. Actually distributed network contains both wireless as well as wired devices; they first need to find whether the frames or packets originally came from wireless local area network or Ethernet connection.

Here two cycles were used Initially, the NTA finds analysis of both ingoing and outgoing data and finds whether an end-station is from Ethernet connection or WLAN connection. In second cycle, the NTA analyses the network load from end-station on wireless local area network to calculate the efficiency. If a wireless local area network end-station generates network load which causes the access point to access the different ports on the gateway router device to which the different access points are associated, then the access action is considered straight-access. If a WLAN end-station generates network load which causes the access point to access the port on the gateway router to which the access point is not connected physically, then the access point action is considered cross-access. If the frequency values of these access point actions exceed a threshold value, the NTA then alerts the network administrator that the end-station is connected to a fake access point.

III. PROBLEM FORMULATION

We have implemented a method in which a wireless devices i.e. mobiles are trying to connect with a Wireless Local Area Network to access the data over the Internet. As all wireless devices scans the complete network or all stations, it looks like there are much more access point in the WLAN communication range now out of all these access points some may be the real access points and some may be rogue access points. Our aim is to design and implement a protocol or algorithm which is definitely going to help the workstations to detect the fake access point. The protocol or the algorithm designed should support in all IEEE 802.11 standard based wireless networks without getting any extra requirements from the network administrator.

Our technique uses a client side method, in which user can prevent connection with a rogue AP. This can be designed with administrator side method in which the system authorities will detect and prevent connection with the fake access points. Consider the two interfaces are used to launch the fake access point using a mobile. the real access point connected with the fake access point by using the first interface, and the access point which is pretending to be the real access point through the second interface. To lure people to connect to it. As soon as the user connects with the fake access point it will send data packets from the second interface towards the first interface, and then toward the real access point. By using this method the user can still be able use the data over the internet as if he associated with the real access point.

IV. PROTOCOL

The protocol simply used to detect the unauthorized access point with the help of complete tour time i.e. statistical timing approach. The concept is that user need to get associate with the network through local server, and finds the total time taken by each request, this process is to be repeated more number of time and response time is recorded of each request. If the calculated mean value is greater than the threshold value then the associated access point is unauthorized access point. In this we are putting the overview of the unauthorized access point detection, following algorithm is to determine whether APoint is unauthorized AP.

Algorithm 1. Detecting Unauthorized Access point (APoint)

1: Start a connection with Access point (APoint)
2: while (i<=n)
3: Pass DNS request to local DNS server
4: Take a log of complete tour time before detection of unauthorized access point i.e. CTT_{Bdet} for 3 or more time
5: Take a log of complete tour time after detection of unauthorized access point i.e. CTT_{Adet} for 3 or more time
6: $CTT_{dev} = CTT_{Adet} - CTT_{Bdet}$
7: if (CTT_{dev} = Positive) then
8: APoint is unauthorized Access Point
9: end while
10: end if

V. IMPLEMENTATION

Hardware description:

Here we demonstrate the infrastructure/hardware required for our project which contains of two access points one of them is legal or authorized access point of company NETGEAR20 (model no- WNR614) and another Access Points

which is laptop itself having hotspot setup and installed as illegal/unauthorized access point, minimum one laptop/desktop machine and two mobile as users, out of two mobiles and two laptop one mobile and two mobiles are legal users who have already registered with original access point or authorized users having all rights of accessing data through NETGEAR20 access point. DNS server of the college network, to find out the side effect of wired network on algorithm.

The specification of hardware used is as follows:

1. Access points. Two access points one from NETGEAR 20 which is secured with WPAPSK2 security, This access point is working with IEEE 802.11 standard and another is laptop on which Hotspot setup is activated
2. Wireless nodes. Laptops/desktop machines and all mobiles with android operating system not necessary android operating system any operating system is applicable.
3. ISP. Broadband internet connection of any service provider

Procedure:

Start the NETGEAR20 access point connect it with the broad band internet connection, this access point is authorized access point. Then configure this access point according to the policy of a service provider. Then connect the laptops and with this access point, so as to form a secure network, i.e. register these nodes or device connected with the NETGEAR20 access point. There may be more machines in the network.

One of the laptop on which is hotspot setup is active i.e. this access point behaving as unauthorized access point. The mobiles phones are trying to connect with network through this access point.

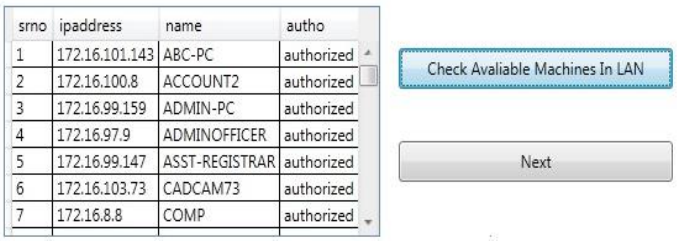


Fig. 1 Name and MAC Address of authorized devices connected With NETGEAR20 Access Point.

Now we have one Netgear20 access point and legal/authorized devices as user of this network. Send the multiple DNS requests to the devices connected with the access point and calculate the complete tour time (CTT) for each request.

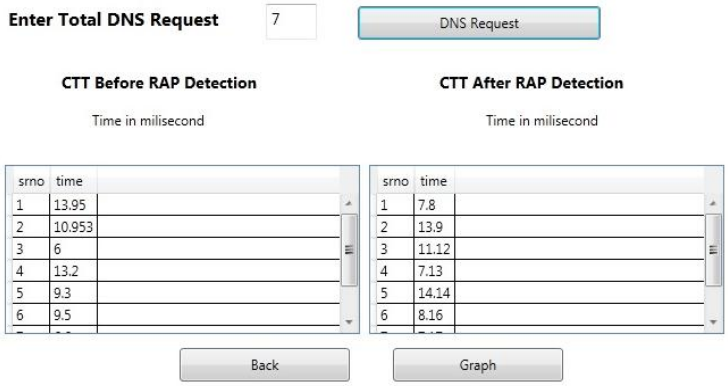


Fig. 2 Complete tour time RTT/CTT after initiating DNS requests to registered devices.

Now any available mobile device is trying to break into the system by hacking the password of the wifi network and connects with the access point installed on the laptop in unauthorized way and pretending to be the legal user of the network, as soon as he succeeded then again after interval we are sending the DNS request to the all nodes connected with the network.

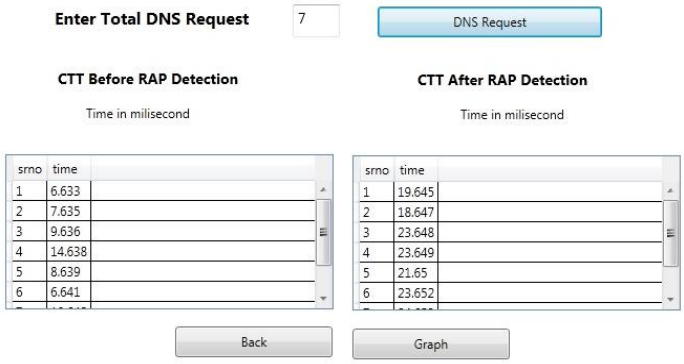
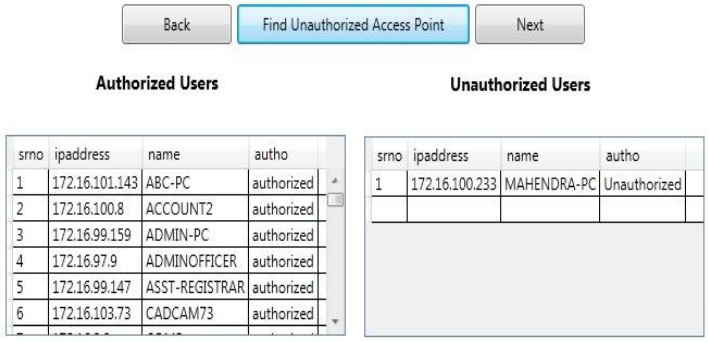


Fig. 3 Complete tour time RTT/CTT detection of unauthorized access point

If we compare the complete tour time(CTT) or round trip time (RTT) taken for processing of DNS request after detection is more than the time taken before detection so we can find the access point trough which nodes are accessing information in an unauthorized way as well as the devices also



srno	ipaddress	name	autho
1	172.16.101.143	ABC-PC	authorized
2	172.16.100.8	ACCOUNT2	authorized
3	172.16.99.159	ADMIN-PC	authorized
4	172.16.97.9	ADMINOFFICER	authorized
5	172.16.99.147	ASST-REGISTRAR	authorized
6	172.16.103.73	CADCAM73	authorized

srno	ipaddress	name	autho
1	172.16.100.233	MAHENDRA-PC	Unauthorized

Fig. 4 Name and IP address of the unauthorized access point

In fig. 4 we can see that on the left hand side all devices displayed are authorized and on the right hand side name and the IP address of the access point which is unauthorized/illegal one.

srno	Unauthorized Access Point	Illegal Devices	Access Timee
15	MAHENDRA-PC	30-C7-AE-1D-22-18	7/5/2015 12:16:53 AM
16	MAHENDRA-PC	30-C7-AE-1D-22-18	7/5/2015 12:26:56 AM
17	MAHENDRA-PC	30-C7-AE-1D-22-18	7/5/2015 12:27:01 AM
18	MAHENDRA-PC	30-C7-AE-1D-22-18	7/5/2015 12:27:06 AM
19	MAHENDRA-PC	30-C7-AE-1D-22-18	7/5/2015 12:27:34 AM
20	MAHENDRA-PC	30-C7-AE-1D-22-18	7/5/2015 12:42:30 AM
21	MAHENDRA-PC	30-C7-AE-1D-22-18	7/5/2015 12:42:31 AM
22	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:38:11 PM
23	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:39:20 PM
24	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:39:25 PM
25	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:39:30 PM
26	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:39:31 PM
27	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:39:35 PM
28	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:39:36 PM
29	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:39:37 PM
30	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:39:51 PM
31	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:39:52 PM
32	MAHENDRA-PC	40-7A-80-30-0B-04	7/4/2015 11:40:30 PM

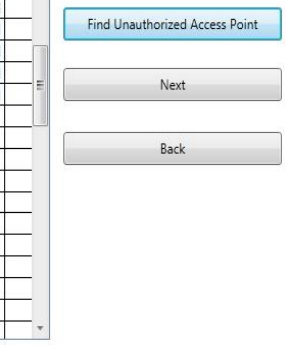


Fig. 5 Name and MAC address of unauthorized access point, device.

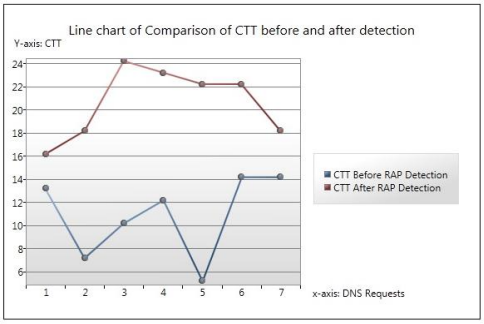


Fig. 6 Line chart comparison of CTT before and after detection of Unauthorized access point

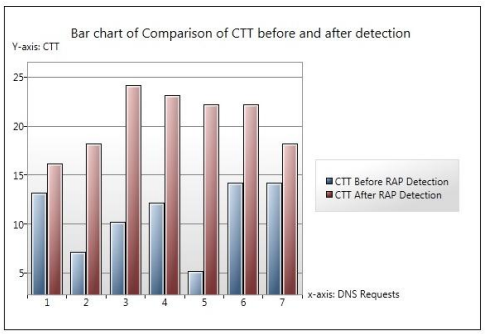


Fig. 7 Bar chart comparison of CTT before and after detection of Unauthorized access point

The fig. 6 & 7. Represents Line chart and Bar chart comparison of CTT before and after detection of unauthorized access point. The blue line represents the values of seven DNS request before detection of intrusion in the wifi network, whereas the red line represents the values after detection of intrusion in the network.

VI. LIMITATIONS AND FUTURE WORK

The limitation of our approach is that some time it may happen that the Request is coming from the legitimate AP and the time taken by the same AP is more than the specified threshold, in this case the connection is broken even if the request is from the legitimate AP. In the future we will focus on finding solution to the above limitation.

VII. CONCLUSION

Here our approach of detecting rogue access point is simply using timing based scheme i.e. Our protocol to detect rogue AP is using a timing based details for the complete time for trip. The intention is that the user Connects to local network through server and the switch and then calculates the complete time for trip from the response. The user repeats the process for a more number of time and store all the time taken at every trip. If the average value calculated is simply larger than the threshold value. Then we can come to the decision that the associated AP is the rogue AP.

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] Qu, G., Nefey M.M.,"RAPid.An indirect Rogue Access point Detection System", IEEE 2010.

[4] Roth, V., Polak, W., Rieffel, E. Turner, T.,"Simple and effective defense against Evil Twin Access Points", WiSec'08, March 31–April 2, 2008, Virginia, USA, 2008.

[5] Chao Yang, Yimin Song, Guofei Gu,"Active User-side Evil Twin Access Point Detection Using Statistical Techniques

[6] Sachin Shetty, Min Song, Liran Ma, Rogue Access Point Detection by Analyzing Network Traffic Characteristics

[7] S. B. Vanjale et al. "Illegal Access Point Detection for Wi-Fi Network by Using Hybrid approach" in International Journal of Advanced Engineering Technology, IJAET, E-ISSN 0976-3945, Vol.II, Issue IV,2011.

[8] S. B. Vanjale, S. Thite "Elimination of Rogue access point in Wireless Network" in International Journal of Scientific & Engineering Research"(IJSER)/Vol.-4/ Issue-12/December-2013.

[9] S.B.Vanjale, S. Thite. "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.

[10] S. Sonawane, S.B.Vanjale "A Survey On Evil Twin Detection Method For Wireless Local Area Network" in International Journal of Computer Engineering and Technology" (IJCET)/Vol.-4/ Issue- 2/March-April 2013

[11] S.B.Vanjale et. al. "Unapproved Access Point Elimination In WLAN Using Multiple Agents And Skew Intervals" in International Journal Of engineering science and Technology, IJEST Vol. 4 , No.02 , February 2012.

[12] S.B.Vanjale et.al. "Detecting and Eliminating Rogue Access Point In IEEE 802.11 WLAN" in International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) vol- 1, Issue-1, 2011.

[13] K. kao, I-En Liao, Y-C Li, "Detecting rogue access points using Clientside bottleneck bandwidth analysis," Science Direct, computers Security 28 (2009), 144-152

[14] T. Kim, H. Park, H.Jung and H. Lee (2012) "Online detection of fake access points using received signal strength"

[15] S. Nikbakhsh, A. Manaf, M. Zamani, M. Janbeglou, "A Novel Approach for rogue access point detection on the client side," International conference on Advanced Information Networking and Applications workshops.2012.

[16] V. Roth, W. P.Polak, E. Rieffel and T. Turner, "Simple and effective Defense against Evil twin access points," WiSec08, Alexandria, Virginia, USA, April 2008.

[17] B. Yan, G. Chen, J. Wang, and H. Yin, "Robust detection of unauthorized wireless access points," Springer, Mobile Network Appl (2009),508-522.

[18] Wei Wei, Kyoungwon Suh, Bing Wang, Yu Gu, Jim Kurose, Don Towsley, Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK-Pairs∗.

[19] B. Yan, G. Chen, J. Wang, and H. Yin, "Robust detection of unauthorized wireless access points," Springer, Mobile Network Appl (2009),508-522.

[20] Sandeep Vanjale, Swati Jadhav, Dr. P.B.Mane "Illegal Access Point Detection Using Clock Skews Method in Wireless LAN", IEEE 2014.

[21] Sandeep Vanjale, Dr. P.B.Mane, Sandeep Mane, "Wireless LAN Intrusion Detection and Prevention System for Malicious Access Point" 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) 978- 9-3805-4416-8/15/$31.00_c 2015 IEEE

[22] Sandeep Vanjale, Dr. P.B.Mane, "A Novel approach for Elimination of Rogue Access Point in Wireless Network" 2014 Annual IEEE India Conference (INDICON) 978-1-4799-5364-6/14/$31.00 ©2014 IEEE

