WIRELESS LAN INTRUSION DETECTION BY USING STATISTICAL TIMING APPROACH

M.K.Nivangune[1], S.B. Vanjale[2], P.B. Mane[3]

[1]*M.Tech. Computer Engg, student, BVDUCOE, Pune, India*
[2]*Ph.D. Research Scholar, Computer Engg, BVDUCOE Pune, India*
[3]*Professor, Department of Electronis Engg, AISSMS's IOIT, Pune, India*

Abstract

Today as we all are habitual of using internet through wired or wireless LAN Networks, but using internet through Wireless LAN becomes harder as the threat of unauthorized access point is increasing day by day. In This paper we are focusing on different types of rogue access points (APs) that are masquerading and attracting people to get associate with them or to connect with them. We are implementing a solution to avoid people or users from connecting to the unauthorized access point by using experimental time dependent scheme.

Our detection technique is a client-oriented method that uses the complete tour time between the DNS server and user that perfectly determine that whether an access point with which the user has connected is the legitimate access point or a unauthorized access point. In this paper we are implementing concept using .Net framework and sql server, Which gives us the characteristics like robust, accuracy and effectiveness for detecting rogue or unauthorized access point without getting any help from WLAN administrator. In this simulation technique we will get accurate values so that we can distinguish between rogue access point and legitimate access point

Keywords— *WLAN, APs, RAP, LAN*

----------***----------

1. INTRODUCTION

During The last few years there is remarkable growth in the use of IEEE 802.11 wireless Local area networks (WLANs). so the use of WLAN for accessing data over the internet creates different network security threats. One of the most challenging threat is unauthorized access points (APs), i.e., illegal wireless access points that are installed in the network without any permission taken from the network administrators. Also some legitimate insiders install the fake access point in their organization network to get more productivity. The rogue APs really creates serious security problems to any organizations secured network. They simply used by the unauthorized parties to potentially break into the network and seal some secure information which will simply destroys that organizations security policy. They simply destroys organizations policy as well as make connection with neighbors which are well equipped access points and degrades the overall network performance.

Two different fake access points can be executed with different devices. The firstly it is wireless router that ia used to connect to the Ethernet card directly on the wall. Secondly the fake access points executed on laptop having two or more wireless cards, one connected to a legitimate access point and the other executed as an access point to get Internet access to WLAN stations. 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.

Our main contributions are as follows

- We have done the analysis of different types of methods to detect rogue Access Points
- We suggested a technique that efficiently detect and prevent rogue Access Points in the network
- We have designed a prototype that can be evaluated by injecting various unauthorized Access Points in our wireless LAN. Our results proved that our technique is effective to detect rogue Access Points in the wireless network.

2. RELATED WORK

The threat of rogue APs is growing so rapidly that attracts the researchers in academic as well as in industry to deal with the problem let's look at some methods, Wei Wei, Kyoungwon Suh, Bing Wang, Yu Gu, Jim Kurose, and Don Towsley found Two different techniques that will be used

to detect fake access points. The initial technique detects fake access points by watching the RF airwaves, it licks the additional information collected at routers. The another technique keeps eye on incoming data at a particular point (e.g. a gateway) and come to decision that whether station is using wired or wireless connection. If station which is determined is not registered or nowhere in the authorization list then the access point attached to this list is considered as a fake access point. This initial technique can have different demerits like accuracy, scalability, adaptability, effectiveness etc,

The second technique may not be having above drawbacks as it is completely based on passive calculation at individual point, it has got scalability just require small amount of efforts and cost for deployment, also this way the design is simple to manage. As we know that the detection in second technique is by WLAN connections, it is useful for detection of layer 2 and 3 fake access points. 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 for fake access point detection. This design approach is actually a solution which can be executed on any router devices in any 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 sub networks. In this paper sachin, Min and Liran has implemented the detection of fake access point depends on traffic at the 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 In first, the NTA perform 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, frequency of straight and cross-access actions. 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.

3. 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.

4. PROTOCOL

Protocol is to detect fake access point using a statistical timing approach or complete tour time. The intention is that the user connects to local network through server and the switch and then calculates the complete time for tour from the response. The user repeats the process for a more number of time and store all the time taken at every tour. 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 fake 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

5. IMPLEMENTATION

Hardware description: Here we demonstrate the infrastructure/hardware required for our project which consists of one Access Points which is laptop itself having hotspot setup and working as access point, and four mobiles as users out of the four mobiles three mobiles are legal users who have already registered with original access point and are authorized users and having all rights of accessing data through laptop which is having hotspot setup and behaving as 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. Hotspot setup is activated on laptop and is secured with WEP security, here the laptop is acting as access point. This access point is working with IEEE 802.11 standard
2. Wireless nodes. All four mobiles with android operating system not necessary android operating system any operating system is applicable
3. USB Dongle. It is used to access internet as wireless LAN of Reliance Net connect+

Procedure: Start a laptop behaving as Access point and initiate a internet connection with reliance net connect+ USB Dongle or any other USB Dongle. Then run the .exe file of project and then start the hotspot setup on the laptop then we have four mobile devices available out of which connect three of them with the wifi zone created by hotspot of laptop. As soon as the connection is established with the wifi just register the MAC address of these mobile devices with database. Then these three mobile devices will become the authorized user of this access point.

srno	username	authorized
1	00-15-AF-BF-36-31	Authorized
2	D4-22-3F-FA-1A-9F	Authorized
3	00-26-C6-7A-57-EA	Authorized

Fig. 1: MAC Address of three authorized devices connected With Access Point.

Now we have one laptop behaving as access point and three legal/authorized mobile 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

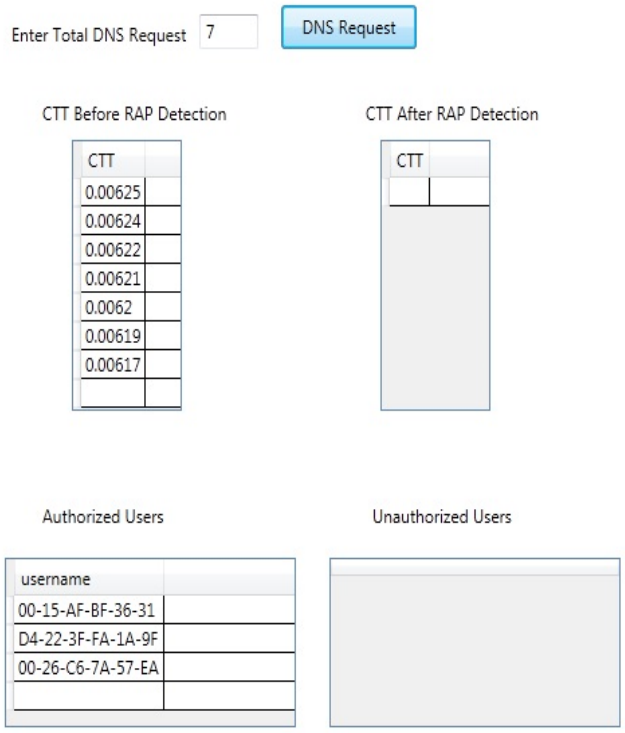

Fig. 2 Complete tour time RTT/CTT after initiating DNS requests to registered devices.

Now fourth available mobile device is trying to break into the system by hacking the password of the wifi network and connects with the access point in unauthorized way and pretending to be the legal user of the network, now again we are sending the DNS request to the all nodes connected with the network.

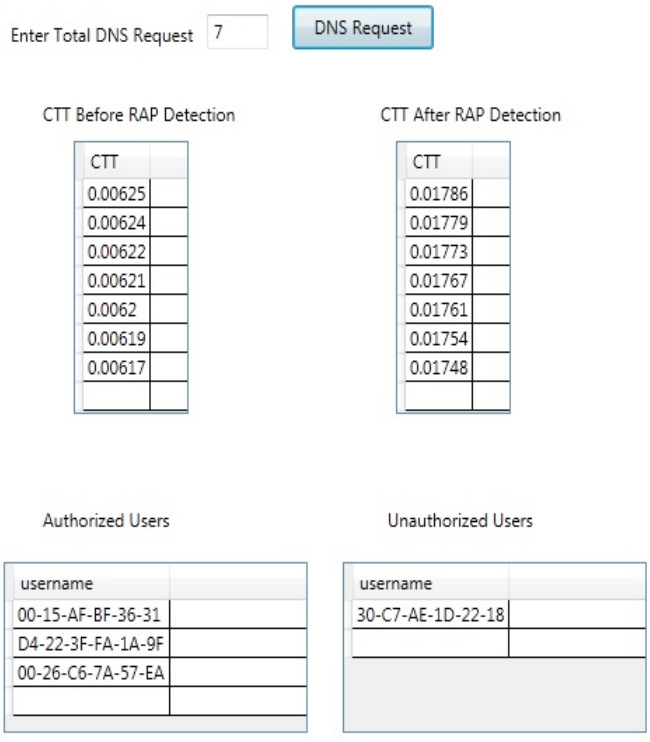

Fig. 3 Complete tour time RTT/CTT detection of unauthorized access point

If we compare the complete tour time(CTT) or round trip time (RTT) time taken for processing of DNS request after detection is more than the time taken before detection so we can conclude that the new device which is detected and whose entry is not there in the database is unauthorized device.

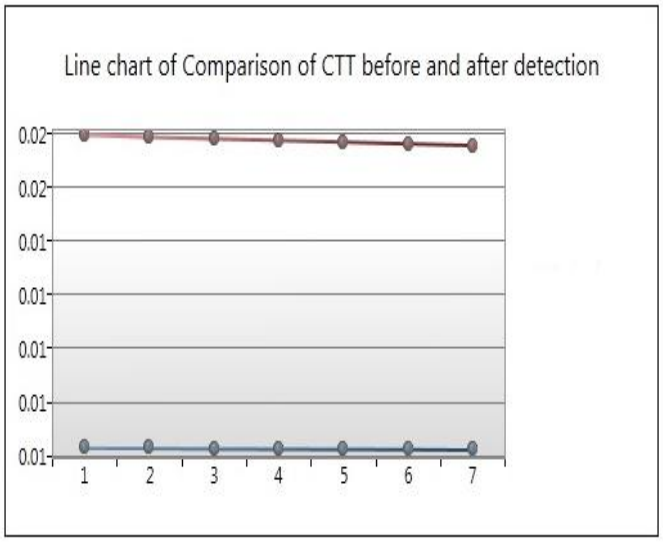

Fig. 4 Line chart comparison of CTT before and after detection of unauthorized access point

The fig. 4. Represents Line 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.

6. 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.

7. CONCLUSION

In this paper 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 Methods 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," ScienceDirect, 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.