Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Wireless Rogue Access Point Detection Using Clock Skew Method

Ms. Swati Jadhav
M.Tech Computer Student
Department of Computer Engineering
B.V.D.U College of Engineering, India

Prof.Sandeep Vanjale
PhD Research Scholar
Department of Computer Engineering
B.V.D.U College of Engineering, India

Abstract*— Rogue Access Point (RAP) is an access point that has been installed on a secure network without explicit authorization from a system administrator. The major security thread for the Wireless Networks is a presence of Rough access points. If this kind of network threats are not detected and mitigated on time, those will lead to the serious network damage and data loss.Finding and avoiding rogue wireless access points is a main issued for every organization. We use clock skew as a parameter of a wireless access point (AP) to detect unauthorized AP's. Using clock skews method to detect Rogue access point in wireless LAN network overcomes the limitations of existing solutions. We calculate the clock skew of an AP from the IEEE 802.11 Time Synchronization Function (TSF) time stamps sent out in the beacon/probe response frames. We use least-square fit method for this purpose. Our results indicate that the use of clock skews appears to be an effective and robust method for detecting fake AP's in wireless local area networks.

***Keywords*—AP, RAP,WLAN,WEP, RF scanning, MAC address, Man-in-middle attack, Clock skew.**

I. INTRODUCTION

Today the Internet has become necessary for connecting with the world. The online market has been growing whether it is in the field of communications, E-commerce, Banking or retail. The end users are very frequently using the internet and using their private identity online, by sharing their data on the internet which can be easily sniffed from the air by using some tools that are available today. Here comes the hard part of using wireless devices in the network, as everyone is using mobile phones, wireless laptops which contain the WLAN card to connect to the access point in the wireless local area network [10].The wireless network is one of the most enhanced sectors because of its flexibility and mobility it is used in every sphere of communications nowadays like business, education or research, so it has become an integral part of life. This technology have certain disadvantages also, there are ways by which air traffic can be sniffed using network interface card in monitor or RFMON mode[12]. A simple example of DOS attack (Denial of service attack) where a legitimate user want to gain access to website on internet but someone is performing denial of service attack on the server side or on his machine due to which end user is unable to get access to the website. There are certain measures one should follow to reduce the possibilities of wireless attacks such as disabling its SSID broadcasting, changing the default SSID and changing encryption mode to WEP (wired equivalent privacy) to WPA2[14]. Today every Wireless LAN card used in laptops has a monitor mode and that can be enabled by using different open source tools that are available in the available in the market. Which can be installed on the laptops and wireless air traffic can be sniffed very easily. Some software like Netstumbler for Windows and Kismet for Linux are used to capture the air traffic of the wireless LAN. Some software like Netstumbler for Windows and Kismet for Linux are used to capture the air traffic of the wireless LAN.

II. EXISTING SYSTEM

Rogue detection is applicable to large wireless networks. It detects the presence of rogue devices in a WLAN network based on the pre-configured rules. In monitor mode, an AP scans all Dot11 frames in the WLAN, but cannot provide WLAN services. As shown in the following figure, AP1 works an access AP, and AP2 works as a monitor AP to listen to all Dot11 frames. AP2 cannot provide wireless access services.

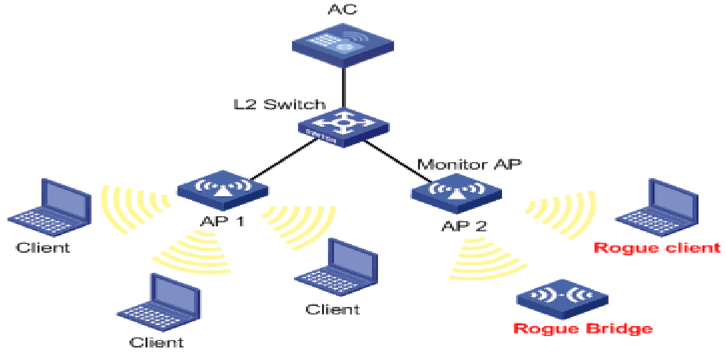

Fig. 1 Monitor AP for rogue detection

One method of detecting rogues involves the use of wireless sniffing tools (e.g. AirMagnet or NetStumber) .

This tool will captureinformation regarding access points that are within range of where tool. This requires you to walk through the facilities to capture the data. With this method, you can scan the entire facility, but this can be very time consuming for larger companies with many buildings or that span a large geographical area.

Capturing data in this fashion is only valid at the time of capture. Someone could activate a rogue seconds after you turn of the sniffing device, and you won't have any idea that it's present. Still, it's often the most common and least expensive method of finding rogues. It just takes a lot of time and effort. The wireless sniffing tools, first list down ccess points that have authorized Medium Access Control (MAC) addresses, vendor name, or security configurations. Then create a list of MAC addresses of the authorized access points on the LAN and check whether or not each you find is on the list.

An access point with a vendor name different than your authorized access points is the first alert to a possible rogue. Improper security settings (e.g., WEP disabled) could indicate a rogue, but it may also be authorized but wrongly configured. Some vendor offer specialized products that provide centralized monitoring. The authorized access points listen for rogues and personnel if a rogue appears, send results to a centralized console that can alert security .This is effective at spotting rogues, but those not within range of an installed access point go undetected. Such systems can be relatively expensive, and they don't work unless you either have or plan to install a WLAN. (Yes, rogue access points can be a problem even if the company doesn't have a WLAN.) If funding is limited or you don't have a WLAN, then using a wireless sniffing tool to manually search the facility periodically likely your best alternative.

Demerits of exiting system:

1 Manual Radio Frequency i.e. RF scanning is lengthy and tedious, which Detect rogue AP only, when scanning is applied. The above effect gives sufficient scope for attacker to attack without getting detected with its purpose of attack. It is the severe drawback of this method.

2 RF scanning approach is the way to problem of scaling of network as it is not easily scalable.

3 RF scanning method is also do impact on the costing and also it is not so effective and accurate.

4 Manual RF scanning is high power consuming.

5 Automatic scanning using lot of sensors is with short time method than manual, also gives the continuous vigilance to rogue AP. But with lot of sensors adds the cost, which is also critical.

6 Automatic scanning depend on signs of APs (viz. MAC address, SSID, etc.) which is ineffective when a rogue AP spoofs signatures.

7 Many time wireless clients are diverted to collect information about the APs which are nearby one, and give the info to centralized server for the detection of RAP. This approach is not effective to spoofing. All unknown APs flagged as rogue APs, which gives the large number of false positives.

8 Mostly dense RF scanning is used for more accurate detection of access point. But it relies on effective operation of a large number of wireless devices, which is really the difficult to manage.

9 Mostly the existing works detect layer-3 or layer-2 rogue access point

III. WIRLESSS SECURITY THREATS AND VULNERABILITIES

The wireless network deployment is very critical in setting up the security of the network. There are many attacks that have been defined and implemented on wireless networks. Ihave described certain known attacks on WLAN[12][11].

a) Invasion and Network resources stealing include unauthenticated use of internet access. If in a network, the clients are filtered on a basis of their MAC addresses, an intruder only has to determine his MAC address and assign some IP address to the wireless device. The intruder will wait until device goes offline from the wireless network, and then the intruder can start using the network resources using the same parameters as a legitimate user.

b) Secondly, an attacker can also divert the traffic and change its path towards the attacking station that he is using in such a way as to steal the packets of those stations, and he can retrieve the information for the data packets.

c) Denial of service attack:

In this attack, the attacker makes computer resources and services unavailable for the end user by targeting the end user machine and its network connection. The end user is not able to use his own services; this attack can be implemented on the end user machine or the server machine. The most common DOS attack is to make the wireless network so much congested with information that the users are not able to access the network resources. Let s take an example: suppose the user types a URL in an internet browser. He is sending a request to the server to view the page. The server can process a limited request in given amount of time. The attacker can overload the server by a sending large number of requests that servercan not process. In that case, the end user will not be able to access the URL as long as the denial of service attack is going on server side.

d) Distributed Denial of Service attack:

In a DDOS the intruder is working with many machines or computers to perform DOS attack. In this scenario, the attacker can gain access to the end user s machine by finding out the security weaknesses. Generally the attacker send large bulk of data to a website or send spam emails to a particular email address so that the system should not be able to respond back, and hence this attack is called as distributed denial of service attack as it is launched from different machine acting together. These attacks can lead to total shutdown of the network, so it is very critical to prevent these kinds of attacks especially for an enterprise or a large company.

e) A rogue access point can be defined as an access point that has been installed by the attacker to intrude or attack the wireless network without authorization of the local administrator. It usually traces the wireless traffic of the client to whom it appears to be a valid authenticator or the end user. The packet captured by the attacker can be held with sensitive information and can be further used for more attacks to exploit the network resources. In my report I have mainly focused on detecting the wireless rogue access point using a timestamp approach.

IV. MAN IN MIDDLE ATTACK

This attack can be performed by two major ways. The First one is eavesdropping, and the second is manipulation. In Eavesdropping, the attacker receives a data stream of the client. It is not considered as a direct attack unless and until any sensitive information is leaked. The attacker can record and analyze the data packets and communication transmission as he can listen, whereas in a manipulation attack, the attacker can receive, change and retransmit the data to the victim machine. I have described in detail both the approach that can lead to a man-in-middle attack [8].

a. Eavesdropping

Wireless communication is not restricted to one particular location, so the attacker has a good chance in tracking down the radio frequency signals of the wireless network, which is an easy task. The tracking of a radio signals is called passive eavesdropping. He can analyze and monitor the data traffic in real time.

Normally the wireless transmission is limited to certain distance because of the limitations of hardware used in access points or Network interface cards with respect to antenna range.

There are devices available on the market today that can read the radio frequency signal from a considerably long distance of a mile or two. This is a security encryption mechanism in wireless LAN called as WEP i.e. data link encryption, which is not secure as various weakness and flaws have emerged. This has been replaced by other encryption mode WPA and WPA2.

Due to the weaknesses that have emerged in wireless networks, more security features have been implemented in WPA and WPA2.

There are certain tools available on the market that can hack the WEP key of the WLAN and break the security.

b. Manipulation

In this approach the attacker can alter and change the data packets and send it to the victim. Moreover, the intruder can collect hidden and important information by installing the Fake AP into the wireless LAN.

The Fake AP would look like a valid access point, since many clients will connect to wireless AP that is having good signal strength by that the user can be easily be fooled by the attacker and all the communication can easily be tracked or monitored through that Fake AP.

This is called as active eavesdropping. The attacker can easily gain access to WLAN without any effort if that network is not password protected.

If WEP is enabled it makes the task of the attacker a little tougher but not impossible as there are many weaknesses in the WEP mode of encryption and various attacks have been implemented with the help of certain war driving tools. The attacker can easily modify the data because ICV (Integrity value check) used by WLAN in CRC-32.

In ICV bits can be flipped easily. The flipped bits can be detected easily by using the CRC method to produce the checksum of modified message.

V. PROPOSED SYSTEM :

The motivation to work on this comes from security issues and attacks that are present with related security risks associated in wireless network. Today in the market there are many war driving tools that are available and used to capture the air traffic. Attackers can use these tools to capture the end users information that can reveal its personal identity and other valuable information. There are security standards that are defined in IEEE for 802.11 protocols. Still there are some attacks that can easily rule out the security of home network as well as enterprise network. There are some open source tools available in Linuxoperating system that can be used to break the security. So the question is: How can we detect when one has become the victim of the attacker. The system is designed which can help the end users to detect the Fake AP on their network and get rid of it. The system works on the principle of LSF (Least Square fitting method).

The wireless network scan using passive approach and gathered the information needed from nearby wireless access point available in the network. The information like its SSID, BSSID, Encryption mode and channel of the required AP is gathered to find out the “timeval” field of each access point from its 802.11 beacon frames and calculates the “clock skew” of each AP. Once that “clock skew” is measured and stored. It is used to check the “timeval” field in next scanning interval again to check whether the AP is Fake or not. The threshold value has to remain fixed once it is calculated. It works on the principle of difference between clock skew. If “timeval” field of same AP has a difference in clock skew and difference is bigger than the threshold then it’s a Fake AP.

This deals with handling the Fake AP on wireless network.

The wireless risk has been increasing very frequently and personal identity of the users is at compromise, if they want to gain internet access.

I have also mentioned some of the counter measures that the end users must follow once it is discovered that it is connected to Fake AP in the last section of the report. The beacon frames captured using a passive scanning approach from the wireless network and extracted the timestamp information from frames to determine its accuracy. The beacon frames has “timeval” field which is used to keep track of the time during communication in the network. Clock skew is calculated by determining the “timeval”field of the beacon frames. Even if the clock skew values are closely associated, it is possible to detect the Fake AP using LSF method.

A Fake AP usually copies the value for “timeval” field from the source beacon frame. It takes nearly the same clock skew from the authorized AP. But when the beacon frame is reconstructed again, the delay of a few microseconds is injected during formation of the frames and its retransmission. This will generate the duplicate frames with different sequence numbers and hence this makes it possible

to detect that the AP is fake.

This approach records the timestamp field and calculates the threshold value in scanning module and detection algorithm records the timestamp interval difference

a. Least Square fitting method

This method works by using best fitting curve of the given type that has minimal sum of the deviation squared (least square error) from the given set of data.

A brief explanation about the method in mathematical form is described below suppose we have some data points *(x1, y1), (x2, y2) ….. (xn, yn)*where *‘x’* is independent variable and *‘y’* is the dependent variable.

The fitting curve *f(x)* has the error deviation *(d)* from each point.

d1 = y1 – f(x1), d2 = y2 – f(x2),………… ,dn = yn – f(xn)

According to this method, the best curve property is highlighted as follows:

$$II = d_1 2 + d_2 2 + \cdots + d_n 2 = \sum_{i=1}^{n} d_i 2 = \sum_{i=1}^{n} [\, y_i - f(x_i) - f(x_i)]^2 = \text{maximum}$$

a. Pseudo code

```
Algorithm of Detect Fake access Point (AP)

Scanning Module
    1. With scanning module system gathers
       beacon packets from select AP.
    2. Maximum value of slope line is
       determined.
       a. Set as threshold of clock skew.
3   Threshold differentiates between frames
from different APs.

Detection Algorithm (AP)
    1. Clock skew and threshold value are saved
       for this phase.
    2. Capture again the desired number of
       packets from each source to determine
       accurate clock skew.
    3. Threshold value helps to separate the
       packets in various datasets.
    4. Apply (Least squaring fitting) on each of
       the dataset to calculate its clock skew.
    5. If you get beacons having same MAC,
       SSID and BSSID but lying in different
       range of clock skew .That is fake AP.
```

Flowchart for Fake AP Detection

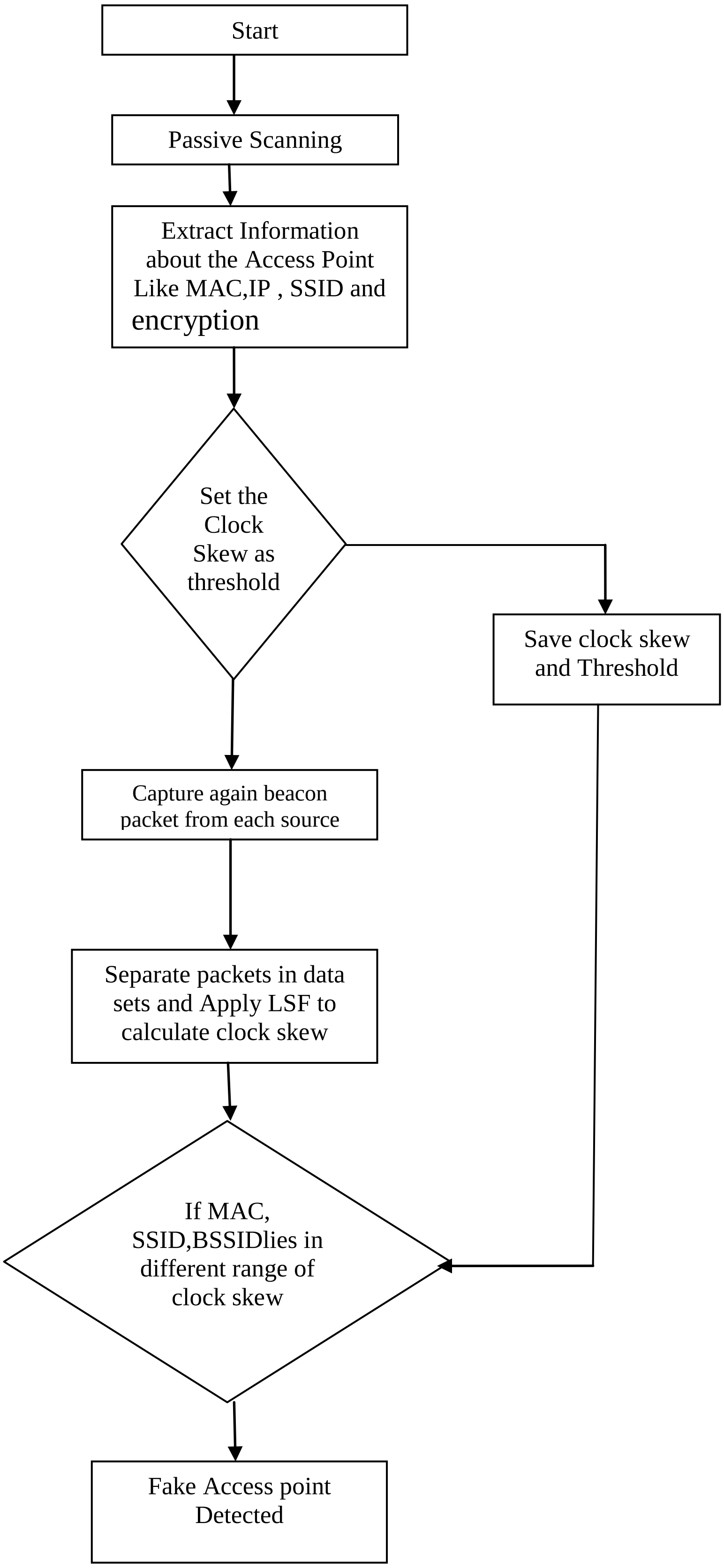
Start
Passive Scanning
Extract Information about the Access Point Like MAC,IP , SSID and encryption
Set the Clock Skew as threshold
Save clock skew and Threshold
Capture again beacon packet from each source
Separate packets in data sets and Apply LSF to calculate clock skew
If MAC, SSID,BSSIDlies in different range of clock skew
Fake Access point Detected

Fig. 2 Flowchart for Fake AP Detection

VI. CONCLUSION AND FUTURE WORK

As technology grows, sophisticated and complex systems are being developed, and the increased use of network resources has increased the concern about wireless security regarding both opportunities and risks. The technology has changed communication in today s arena. In the technical field today, powerful tool has been built that can easily breaks, the security of any home or enterprise network.

Today everyone wants to remain connected to the global internet to get the latest updates on the news, entertainment, stock markets, etc. It is easy to access the internet now days through electronic gadgets. But they are not concerned about the weakness of the wireless networks. I have mainly focused on identifying wireless vulnerabilities and security threats for the end users and finding solution to combat them. This work provides solution for the problem of how to handle it. Some of the future work. I want to do in this, to enhance the features of the research work line such as developing and implementing an independent location finding techniques to track down the location of the wirelessdevices with other parameters.I also would like to make a complete intrusion detection system by implementing more detection programs for different attacks available on WLAN.

REFERENCES

[1]. "How thing works: WLAN Technologies and security Mechanisms" http://www.sans.org/reading_room/whitepapers/wireless/things-workwlan-technologies-security-mechanisms_1301

[2]. Threats to Wireless Local Area Network (WLAN) and Countermeasures" ,A.V.Dhaygude, K.R. Patil, A.A.Sawant ,ICONS'07,January 27-29,2007,Erode,Tamilnadu,India.

[3]. B.Forouzan, Data Communicat ion and Networking, McGraw Hill, Fourt h Edit ion.

[4]. Potential Security Threats of a wireless network http://www.infosecwriters.com/text_resources/pdf/Wireless_JMeyer.pdf

[5]. Suman Jana and Sneha Kumar Kasera. On fast andaccurate detection of unauthorized wireless accesspoints using clock skews. In *MobiCom '08:Proceedings of the 14th ACM international conferenceon Mobile computing and networking*, pages 104–115.ACM, 2008.

[6]. Sushama Shrike, S. B. Vanjale, B.V.D.U, Pune (ROGUE ACCESS POINT DETECTION USING TIME STAMP) Jun-2011 vol 2.

[7]. The Method of Least squares: http://www.efunda.com/math/leastsquares/leastsquares.cfm

[8]. Man-in-the-middle attack- the IT Law wiki: http://it.toolbox.com/wiki/index.php/Man-in-the-Middle_Attack

[9] . Wikipedia Man in Middle attack: http://en.wikipedia.org/wiki/Man-in-the-middle_attack

[10]. Wikipedia (Wireless LAN): http://en.wikipedia.org/wiki/Wireless_LAN

[12]. Security Standards: http://www.sans.org/reading_room/whitepapers/wireless/overview-80211-wireless-network-security-standards-mechanisms_1530

[11]. Wireless LAN: Security Issues and Solutions: http://www.sans.org/reading_room/whitepapers/wireless/wireless-lan-security-issues-solutions_1009

[13]. Wireless security: http://en.wikipedia.org/wiki/Wireless_security

[14]. WEP (Wired equivalent Privacy): http://www.networkworld.com/details/715.html

[15] Lanier Watkins, RaheemBeyah, Cherita Corbett "A Passive Approach to Rogue Access Point Detection" 1930-529X/07/$25.00 © 2007 IEEE

[16] SongritSrilasak,,KittiWongthavarawat and Anan Phonphoem, Intelligent Wireless Network Group (IWING*)* "Integrated Wireless Rogue Access Point Detection and Counterattack System" published in 2008 International Conference on Information Security and Assurance.

[17] "AirMagnet:EnterpriseWLANmanagement."[Online] Available: http://www.airmagnet.com/

[18] . NetStumbler, http://www.netstumbler.com.