Elimination of Rogue access point in Wireless Network

Mr. Sandip Thite, Prof. Sandeep Vanjale, Prof. P. B. Mane.

Abstract— Now a day's in many public places like bus stations, restaurant, malls etc. provides Wi-Fi connectivity to the users with free of cost. These public places having a device like wireless access point through which they provide service to the end users. The growing acceptance of wireless local area network causes a risk of wireless security attacks. The attacker creates a rogue access point to attract the users and perform attacks on user devices through WLAN. Detection of a rogue access point (AP) is a big challenge for network administrator. Presence of rogue access points is serious threats which steal sensitive information from the network. Deploying access points and restricting the use of these access points to authorized users has been a challenge due to the weak authentication and encryption used in wireless standards. There are many techniques which provide a solution to this problem. Most of these solutions are automated and are dependent on a specific wireless technology. In this paper we have presented a survey on existing techniques with its merits and demerits.

Key words— Fake access point, IEEE 802.11, Man-In-Middle attack, Malicious attacker, Rogue access point, wireless security, WLAN

1. INTRODUCTION

The increase in the number of mobile Smartphone users in the world has been impressive. There is a rapid growth of the users who used the WI-FI through mobile devices. Specially device like Tablet are connected only through Wi-Fi. All these devices connect to wireless network through a device called as the Wireless Access point (WAP). The access point is very popular because of features like it is scalable, cost effective, easy to install, easy to configure and the more important it provides mobility.

The use of public Wi-Fi has reached at the level that it is difficult to avoid. Kaspersky [1] conduct a global poll through Facebook about Wi-Fi security, and the result shows that more than 32 % of users said that they used public Wi-Fi regardless of the security concern. A malicious attacker creates a rogue access point in a wireless environment. The main target of these attackers is to disturb the network and try to steal sensitive information.

If the rogue access point is undetected then it is an open door for an attacker to get sensitive information. Attackers take the advantage of undetected rogue access points to get a free internet, confidential information. If a rogue AP is added to the network, it must be discovered and the necessary measures must be taken to rectify the situation. According to AirTight Report [2] out of total access points 20% access point is unauthorized in network and users can easily connect to these access points because of lack of knowledge about security threats in WLAN. Figure 1 shows that scenario.

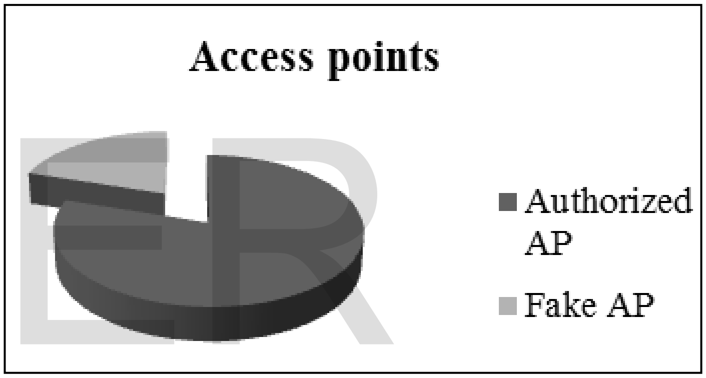

Figure 1: Authorized AP vs. Fake (Rogue) AP

Rogue access points [3] are easily deployed, hard to detect, and open enterprise networks to a variety of attacks. It performs two types of attacks-Passive and active attacks. In Passive attack attacker don't affect the normal behavior of the network. Even network users are unknown about the attack. Attacker steals the confidential information without knowing the user while in active attack; attacker affects the normal behavior of the network. The most common active attacks are Denial of service, Man-in-Middle attack and session hijacking attack.

This paper focuses on important security issues of wireless network which is called as Rogue Access point. This rest paper of the paper organized as follows. Section II describes background details of access point. Section III describes literature survey about rogue access point detection technique. Proposed system presented in section IV. And finally we conclude in section V.

2. BACKGROUND

Access point

Wireless Network cannot complete without Wireless access point (WAP). It is a central controller for the wireless de-

- *Mr. Sandip S.Thite is currently pursuing masters degree program in computer engineering in Bharati Vidyapeeth Deemed University Pune,India, PH-+99850988672. E-mail: sandip_thite@yahoo.co.in*
- *Prof. Sandeep Vanjale is Ph. D. Research scholar in computer engineering in Bharati Vidyapeeth Deemed University Pune,India, PH-+919422040905. E-mail: sbvanjale@bvucoep.edu.in*
- *Dr.P. B. Mane, Professor, Department of Electronics & Telecommunication in AISSMS IOIT, Pune, India, E-mail:Pbmane6829@rediffmail.com*

vices. It takes the services from the wired network and provides it to the different wireless devices. Infrastructure development cost is very low because of no use of cables for connecting with wireless devices. By using a single access point we can easily connect to a multiple wireless devices. The hotspot is a very famous application of WAP. Attacker can create a hotspot using its own wireless device which acts as a rogue AP [4] and attracts other wireless devices and performs attacks on those devices.

Wireless traffic encryption technique provides a security to wireless network using the wireless encryption protocol. Latest access points come with a built in wireless traffic encryption technique. But the tools like Aircrack-ng suite can be used by attacker to break the security of wireless network by monitoring wireless traffic [3].

The unauthorized access point is divided into two categories-

1. Rogue Access point – the term rouge AP has been used in more than one context in wireless security literature. It is installed or set by not only by the outside attacker but also authorized user on the network to take a more advantages of the network.

2. Fake Access point [5]– It is set or installed by an outside attacker without knowing to an authorized user of the network. It is set up by a malicious attacker for the purpose of malicious behavior such as falsification, eavesdropping, steals the information.

It is easy to create a rouge AP. As illustrated in figure 2, malicious users configure his own device (Laptop, Tablet) by using some software available in the market. After creating a rouge AP attacker wait for a client node to connect to that rouge AP or sometimes actively send multiple signals to client node and force him to change the connection. Even it analyzes the wireless traffic using tools like Aircrack-ng suite. It captures the beacon and management frame and try to get nodes MAC address Logical address and Service set Identifier (SSID). By this way it performs attack on client nodes. Without creating an additional network connection it uses the internet services for wired network through authorized AP and provides it to client node. By this way a malicious attacker steal the personal information of client node without knowing the client.

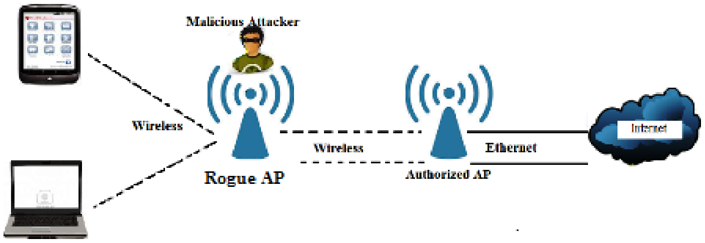

Figure 2: An example of rogue AP Attack

Network users have the misconception that if we have a firewall then don't worry about Fake AP. But it is wrong. The firewall installed in between LAN & WAN. If a rogue AP created by the attacker within LAN then firewall does not detect the rogue AP and also does not see the traffic through rouge AP. Even WPA2 cannot protect a network from rogue AP. We can enforce the security controls such as WPA2 only on managed or authorized AP. Rouge AP is the unmanaged AP so we cannot enforce security control to it. Even rogue AP threats work at a layer below wired intrusion detection system & antivirus so even it is not useful for detection of rogue AP.

3. LITERATURE SURVEY

There are a number of existing techniques are available for the purpose of detection of Rogue AP. These techniques divided into categories like traditional approach, client side, server side and hybrid approaches.

The traditional approach is based on the concept of matching. It verifies the access point attributes which include the MAC address of the AP, if AP is configurable then its logical address. It also verifies the SSID. If all these attributes are same then it conclude that it is authorized AP. But now a days traditional approach is not sufficient for the authentication of authorized AP. In market there are a number of tools available which can be used for identification of MAC and logical address. Even by analyzing the wireless traffic we can easily get these things. So traditional approach is not sufficient in the current internet world.

In server side approach, it is a central controller of the wired and wireless network. It monitors both the network by using software tools. For detection of rogue AP, Rogue AP detection software installed on a centralized server and by using this software it analyzes the whole network and performs some specific operation for detection of rogue AP. It continuously monitors the network, if any misbehavior finds on the network, it checks the status of that particular AP to decide whether that AP is legitimate or not.

The client side approach [6] is challenging because there is no prior information about network which can be used as a reference. Even client doesn't know about the authorized access point list. Even nodes don't have any sophisticated software tool available within it. There are a number of ways to secure a client node in a wireless environment. It takes the services from server for detection of rogue AP. Some client node has a pre-installed software on their device, which continuously monitor the network and before connecting to an access point it verifies all the details of access point to judge that access point is authorized one or not.

There is a research going on to find a good technique for rogue AP detection. Industry people and academic researchers are both works on to find a better solution for the detection of Rogue AP. Existing research techniques uses different parameters such as clock skew, wireless traffic monitoring, encryption, authorization, timing based approach [14], received signal strength analysis [5], bottleneck bandwidth analysis, and sequential hypothesis test. These techniques are based on client side, server side or hybrid approach. Every approach has some merits and demerits. Some technique is only useful for detection of rogue AP. Prevention is not possible with them.

There are some techniques which focus these problems. Every technique uses different parameters to get a solution which causes a different rate of success for fake AP detection.

There is some industry solution for detection and preven tion of rogue AP. These solutions are as follows-

Air Defense [7] provide a complete software & hardware system which contain sensors deploy throughout the network. Network manager handles the software tool through the management console. It detects malicious attacker and attacks and also detects vulnerabilities in the network. A very slow response time for detection of rogue AP, that is the biggest drawback of this tool and important one is that it is a commercial product.

AirMagnet [8] is another commercial product which is used for detection of vulnerabilities and intrusions. It detects unauthorized APs and denial of service attacks by flooding. But this software product requires a technical person to move around the network for detection of security threats.

Jana et al. [9] proposed a server side solution using clock skews of access point. They used clock skews as a fingerprint to differentiate fake AP with beacon frames. This approach cannot detect MAC spoofing and also it has a lack of accuracy and speed in the calculation of clock skews in TCP/ICMP. There is no provision for lightweight solution. It measure the effects of temperature variations and Network Time Protocol (NTP) synchronization on clock skews. Clock skews are acting as fingerprint so will be unique to each access point.

Kindberg et al. [10] proposed server side model which provides a security to public WI-Fi network. It uses standard encryption and authentication technique with some modifications. This method allows the authorized user to authenticate the access point in a wireless network.

Shivraj et al. [11] present a server side Hidden MarKov Model (HMM) based approach to detect unauthorized access point. This technique uses variation in packet inter arrival time to differentiate between authorized access point and unauthorized access point. It provides average detection accuracy more than 80%. It is easy to manage and maintain. It requires minimal effort and deployment cost. But this technique requires too many trained data for detection and also it works for only specified Denial of Service attack.

Kim et al. [5] proposed client side approach using the concept of received signal strength (RSS) for fake AP. In this method they find highly correlated RSS sequences that can be collected in the wireless device. After that they normalized the received signal and classify whether the collected signal is multiple or not. For that they use a sequential hypothesis technique. It is a lightweight solution to overcome the drawbacks of the client side approach. But in this technique they never consider a distance between the client node and access points while calculating the signal strength. Distance affects the signal strength.

Kao et al. [3] proposed client side rogue access point detection technique using bottleneck Bandwidth analysis. It uses a passive packet analysis approach. It is based on bandwidth estimation using packet pair technology. They also proposed another approach called as client side bottleneck bandwidth with sliding window to get better accuracy with detection technique. But this technique has a problem about how to reduce the size of the sliding window. Packet analysis requires a sophisticated algorithm design which can be quickly deployed to protect the entire network.

Liran Ma et al. [12] implement hybrid approach which contains a model for unauthorized access point detection which includes packet collector, unauthorized access point preemption engine and detection engine. It provides a cost effective solution. Its open architecture allows extra features can be easily added in future. This model follows the traditional approach for fake access point detection which has a many pitfalls.

4. PROPOSED SYSTEM

Rogue AP detection is a challenging task. Current techniques are available for man in the middle attack and evil twin attack.[13] Currently available techniques will not work for every scenario. Some techniques only used for detection, no prevention policy present with these techniques.

We proposed a novel approach which considers Mac address, SSID and signal strength of the access point for deciding current access point is rouge AP or not.

In this technique initially we need to filter 802.11 packets. For that we must capture the packets during wireless traffic analysis. We can use Aircrack-ng i.e. freely available software tool. It is used to analyze the wireless traffic and to capture a packet. By using that we can filter all the wireless network packets and capture beacon and management frame. If packet subtype is 0 then it contains management frame and if it is 8 then it contains a beacon frame. There are some AP who blocks beacon frame so that here we consider both beacon and management frame.

A packet contains a header field. It contains an address filed which stores a physical address of the AP. We can use a received signal strength indicator (RSSI) for the detection of rogue AP. Here we consider an RSSI level in between -100 and 0. Where 0 means the device was exactly at the place of detector and -100 means it is very far away.

We also have an authorized access point list called as a whitelist which contain detailed information of each AP which include specific address logical address and physical address of the AP. It also includes the information about SSID and RSSI of AP.

There are a number of scenarios from that we can find that whether rogue AP present in the network or not.

1. If we found the same physical address for more than one device then we can conclude that rogue AP is present in between these two devices.
2. If we found the same specific address for more than one device then we can conclude that rogue AP is present in between these two devices.
3. If we found same SSID for more than one device then we can conclude that rogue AP is present in between these two devices.
4. We also check the RSSI value. If the RSSI value is same as the previously calculated value, then we consider it as an authorized AP. Even the value is near to that value we consider it as an authorized AP. For example if for one access point we have an RSSI value -50 in our whitelist. But it shows the value around -55, even after that we consider it as an authorized AP.

And if it shows value like -90. It means that there is a chance of rogue AP present in the network.
5. If the particular access point continuously sends a multiple signal then we want to check that whether the access point is rogue or not.

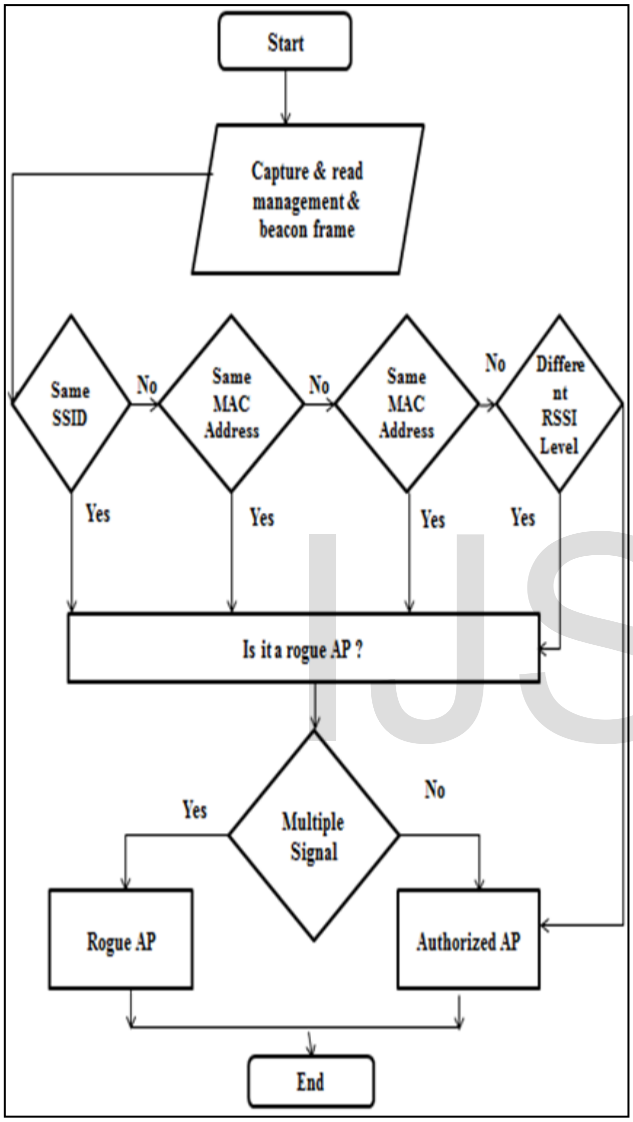

Figure 3: Rogue AP Detection Algorithm

If any access point detected as rogue then node can perform denial of service attack on that access point. So that node will not connect to that access point. It is the best prevention policy to avoid a rogue access point.

5. CONCLUSION

The rogue access point detection system has been a major research area because of increased use of wireless network. In this paper we proposed a novel approach for detection of rogue access point. The proposed system is a kind of wireless intrusion detection system. It uses Hybrid approach. Existing techniques does not provide a lightweight solution. But proposed approach considers all the parameters while detection and provide a lightweight solution without modifying network architecture. The solution is cost effective, scalable and deployable on any network. This techniques works on signal strength. Signal strength can be affected by environmental condition which gives false value of signal strength. So there still remains considerable scope for future research.

REFERENCES

[1] http://blog.kaspersky.com/do-you-use-free-wifi-hotspots-a-survey

[2] Airtight Network Report, 2009 WiFi Rogue Access Points.

[3] K. kao, I-En Liao, Y-C Li, " Detecting rogue access points using client-side bottleneck bandwidth analysis," ScienceDirect, computers & security 28 (2009),144-152

[4] Raheem Beyah, Aravind Venkataraman, "Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions," IEEE Security & Privacy, vol. 9, no. 5, pp. 56-61, Sept.-Oct. 2011

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

[6] 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

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

[8] Airmagnet. Available: http://www.airmagnet.com

[9] S. Jana S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," in Proceedings of the 14th ACM international conference on Mobile computing and networking, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp.104–115.

[10] T. Kindberg, J. Mitchell, C. Bevan, and O'Neill, "Authenticating public wireless network with physical evidence,"IEEE International Conference on Wireless and Mobile Computing, Networking and communication,2009.

[11] G. Shivraj, M. Song and S. Shetty, "A hidden markov model based approach to detect rogue access points" IEEE, 978-1-4233-2677,2008.

[12] L. Ma, A. Y. Teymorian, X. Cheng, "A hybrid rogue access point protection framework for commodity Wi-Fi networks," Proceedings of IEEE INFOCOM 2008.

[13] A. Panch and S.K. Sing, "A Novel approach for Evil-Twin or rogue AP mitigation in wirless environment. International Journal of security and its Applications. Vol. 4, No. 4, October 2010.

[14] H. Han, B. Sheng, C. Tan, Q. Li,and S. Lu "A timing –based scheme for Rogue AP detection," IEEE Transactions on parallel and distributed systems, vol. 22, no-11, November 2011