Detection of Rogue Access Points present in the WLAN (Wireless Local Area Network)

SHIVARAJ ASHOK PATTAR
Dept. of Information Science and Engineering,
BMS College of Engineering
Bangalore, India
pattarshivaraj@gmail.com

***Abstract*—A Rogue Access Point is a wireless access point that has either been installed on a secure network without explicit authorization from a local network management or has been created to allow a cracker to conduct a man-in-the-middle attack. Rogue Access Points (RAPs) that pretend to be legitimate APs to lure users to connect to them. Two types of rogue APs can be set with different equipment. The first type uses a typical wireless router connected directly into an Ethernet jack on a wall. The second type of rogue APs are set on a portable laptop with two wireless cards, one connected to a real AP and the other configured as an AP to provide Internet access to WLAN stations. Many algorithms proposed to detect the rogue access point detection but some of them are time consuming and some of them are expensive. And maximum algorithms are work at client side only. Running client side detection program is not preferable every time. It is better to detect unauthorized access points from administrative side. This paper introduces a better approach to detect the rogue access point detection at the server side.**

Keywords*— *Rogue Access Point (RAP), Wireless Access Point (WAP). Wireless Local Area Network (WLAN).

I. INTRODUCTION

A Rogue Access Point is a wireless access point that has either been installed on a secure network without explicit authorization from a local network management or has been created to allow a cracker to conduct a man-in-the-middle attack. Rogue Access Points (RAPs) that pretend to be legitimate APs to lure users to connect to them. It is necessary to detect the RAP. Rogue devices are an increasingly dangerous reality in the insider threat problem domain. Industry, government, and academia need to be aware of this problem and promote state-of-the-art detection methods.

In computer networking, a wireless access point (WAP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a router (via a wired network), and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.

II. ROGUE AP SCENARIO

With the increasing popularity of Wi-Fi networks, securing such a network becomes a challenging problem. Commodity Wi-Fi networks are particularly vulnerable to attacks because of factors such as open medium, insufficient software implementations, potential for hardware deficits, and improper configurations. Among all the security threats, one of the most dangerous hazards is the prevalence of rogue APs. A rogue AP is typically referred to as an unauthorized *AP* in the literature. This type of device can be easily deployed by end users. When a rogue AP is connected to a network, it can be used by adversaries for committing espionage and launching attacks. Similarly, improperly configured APs and phishing APs can introduce the same security threats once exploited by adversaries. Therefore, they can be regarded as rogue Aps as well. More importantly, there is a more insidious type of rogue APs, called the *compromised APs*, that has drawn little attention in the literature. A compromised AP is the most dangerous rogue AP that can exist in commodity Wi-Fi Networks. In particular, it is difficult to detect such a rogue device because the AP itself is not malfunctioning (e.g., operating without specified security controls). Further, the AP does not display anomalous misbehaviour such as broadcasting a duplicate SSID. Thus, a compromised AP can significantly diminish the overall security of the network. A summary of the types of rogue APs and a number of possible scenarios is shown in Table 1.1 for a detailed taxonomy of rogue APs.

Table 1.1 Taxonomy of rogue APs.

Rough AP Class	Possible Scenarios
Improperly Configured	Insufficient security knowledge; faulty driver; physically defective; multiple network cards
Unauthorized	connected to internal LAN without permission; external neighbourhood AP
Phishing	fabricated by adversary
Compromised	disclosure of security credentials

According to 802.11 standard, when multiple APs exist nearby, a WLAN client will always choose the AP with the strongest signal to associate. To attract clients, therefore, a rogue AP needs to be close to clients so that its signal can be stronger than other legitimate APs.

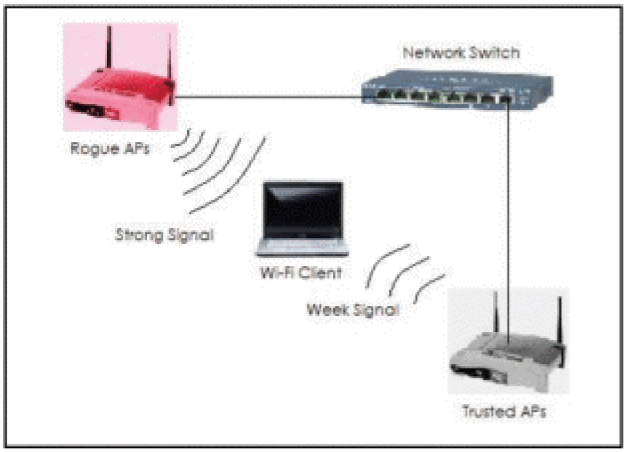

Fig 1. How Rogue AP will provide Strong Signals

In practice, a rogue AP needs further configuration to avoid easy detections, such as spoofing MAC address, SSID, and vendor name, setting up a DHCP server to assign valid IP addresses to connected clients.

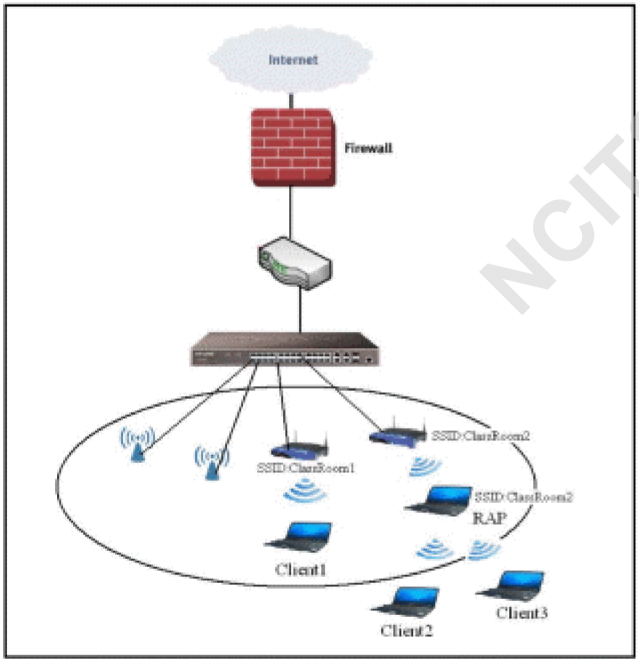

Fig 2. How Rogue APs will be installed by the unauthorized persons.

Identity verification can be done at the client side by using *traceroute* command. But this not helpful when rogue access point is connected to LAN as shown figure 2. The rogue access point will say that it is a gate way for the network.

III. A ROGUE ACCESS POINT

It is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can ignorantly or maliciously install an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network.

To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points. Presence of large number of wireless access points can be sensed in airspace of typical enterprise facility. These include managed access points in the secure network plus access points in the neighborhood. Wireless intrusion prevention system facilitates the job of auditing these access points on a continuous basis to find out if there are any rogue access points among them.

In order to detect rogue access points, two conditions need to be tested:

- whether or not the access point is in the managed access point list
- whether or not it is connected to the secure network

Wireless security

It is the prevention of unauthorized access or damage to computers using wireless networks. Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

One of the most challenging security concerns for network administrators is the presence of rogue wireless access points. A rogue access point (RAP) is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network management or has been created to allow a cracker to conduct a man-in-the-middle attack. The rogue access points are devices that are deployed insecure WLANs without permission or knowledge of the network administrator. The presence of such rogue access point poses severe threats to the WLAN security as it could

compromise security of the entire wireless LAN. This problem has been in existence ever since WLANs have become popular in commercial applications. There have been reports of data theft, identity theft by using these rogue access points. Increasing use of wireless technologies by defense establishments along with above mentioned reasons have compelled researchers all over the world to find a solution for this problem. WLANs face the same security challenges as their wired counterparts, and more.

Need for Rogue Access Point Detection in IEEE 802.11

Within a properly secured WLAN, rogue access points are more damaging than rogue users. Unauthorized users trying to access a WLAN likely will not be successful at reaching valuable corporate resources if effective authentication mechanisms are in place. Major issues arise, however, when an employee or hacker plugs in a rogue access point. The rogue access point helps an attacker in gaining access to sensitive information of an organization. Employees have relatively free access to a company's facilities, which makes it possible for them to inadvertently (or mischievously) install a rogue access point. An employee, for example, installs his personal access point without permission of network administrator in order to support wireless printing or access to the network from a conference room. Software programmers working on wireless applications may connect an access point to the corporate network for testing purposes.

In order to avoid this situation, it is necessary to implement security policies that mandate conformance with effective security controls and coordination with the network administrator before installing access points. This can only be effective, nonetheless, if you clearly inform employees of the policies. After performing several security audits, it has been found that employees often install rogue access points without knowing the company security policies or the consequences of violating the guidelines. A hacker can install a rogue access point to provide an open, non-secure interface to a corporate network. In order to do this, the hacker must directly connect the access point to an active network port within the facility. This requires the hacker to pass through physical security; however, that's easy to do in most companies. Therefore there is an urgent need of developing technology which will address this problem of rogue access points.

RELATED WORK

Common Approaches to Rogue AP Detection

The only way to reliably discover rogue APs is to listen to the airwaves – the wireless side of your network in combination with the wired side of your network. There are software and hardware products that make the former possible, but on their own they offer incomplete solutions.

Sniffers.

One way to find a rogue access point is to search your facility from the wireless side. Sniffer software (such as AirSnort or NetStumbler) allows you to carry a laptop or PDA around your facility scanning all radio frequency (RF) channels for connections with any and all access points within range. While this software allows you to capture valuable information about the access points in your environment, it can be very time consuming to walk through all of your facilities in search of rogues. And data captured this way is only a sample snapshot – only valid when it is captured. Further, you must determine whether the unrecognized access points you discover are rogue (within your facility whether connected to your network or not) or simply foreign (operating within range of your airspace, but connected to some other network, i.e. a neighboring business). While this type of RF audit is often worthwhile, it is costly, incomplete, and too intermittent to continuously protect your wired network from rogues. And if your network covers many geographically dispersed locations, this method of rogue detection may be unworkable.

Probes

To ensure continuous vigilance for rogue APs, you can install full-time probes – electronic devices that continuously monitor all Wi-Fi (802.11) traffic within their range. This can be an expensive proposition. Not just in the cost of the probes (typically $500 to $1000 per device), but also in terms of pulling Ethernet cable and providing electrical power.

PROBLEM FORMULATION

Consider a scenario when a wireless station tries to join a WLAN to access the Internet. After scanning the channels, the station will discover multiple APs within its communication range. Some of these APs are legitimate and some might be rogue APs. Objective is to design an algorithm that helps the station to detect the rogue AP. The detection algorithm should function in all IEEE 802.11-based wireless networks without requiring additional modifications from the network administrator. Proposed scheme uses a client-centric approach, where a user can avoid connecting to a rogue AP. This can be combined with administrator-centric approaches where the system administrators actively detect and disable rogue APs. It is assumed that the rogue AP will be launched using a mobile device with two wireless interfaces. The first interface connects the rogue AP to the legitimate AP. The second interface pretends to be a legitimate AP to induce users to connect to it. When a user associates to the rogue AP, the rogue AP will forward packets from the second interface to the first interface, and then toward the legitimate AP. This way, the user will still be able to access the Internet as if connected to a real AP. Fig. 2 illustrates the setup.

PROPOSED SYSTEM.

Rogue AP detection algorithm uses timing information based on the round trip time. The intuition is to let the user probe a server in the local network and then measure the RTT from the response. The system admin repeats this process for a number of times and records all the RTTs. If the mean value of RTTs is statistically larger than a certain threshold, we regard the associated AP as a rogue AP. It is begin with

examining the motivation and challenges of rogue access point detection.

Algorithm to detect whether AP_x is a Rogue AP or not.

Algorithm 1: Detection of Rogue Access Point (AP_x)

1: Collect request to connect to the server.
2: Accept Connection request from AP_x
3: for i=1 to n do
4: send unicast probe to AP_x record the round trip time(RTT_{probe})
$RTT_{probe}=RTT_{probe} - T_{data}$ (probe)
5: End for
6: Filter out outliers.
7: RTT_MEAN_{probe}=mean of remaining RTT_{probe}.
8: SD_RTT_{probe}=Standard deviation of remaining RTT_{probe}.
9: $D_t= RTT\_MEAN_{maintained} - RTT\_MEAN_{probe}$
10: $V=f(SD\_RTT_{probe}, SD\_RTT_{maintained})$
11: if($V>D_t$) then
12: AP_x is a Rogue AP.
13: End.

$V=f(SD\_RTT_{probe}, SD\_RTT_{dns})$

$$=$$

$$A+\left(\frac{SD\_RTT_{probe}+SD\_RTT_{maintained}}{2}\right)+B \quad (1)$$

Where A and B are parameters depending on network line connections.

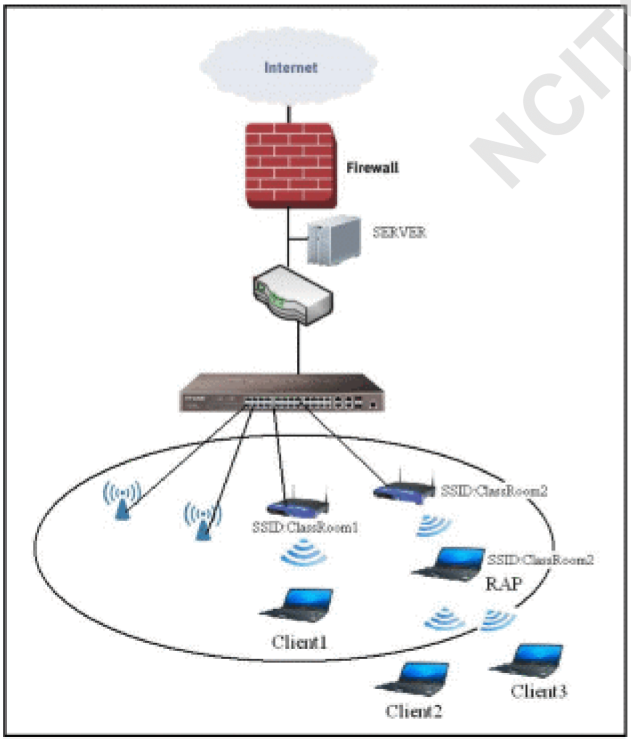

Fig 3.Proposed system diagram.

As discussed in the above algorithm the server will send ping requests to all systems connected to it and collects all round trip times (RTT). Whenever server pings, server will collect the MAC addresses and IP address of all network elements in the network. If the difference of calculated RTT and threshold value of maintained RTT exceeds then it is treated as a suspicious access point. Then the collected Mac addresses will be compared with pre-maintained MAC address table. If MAC address matches with anyone address of the table then it is not a rouge access point. If the MAC address does not match then it is a rogue access point. And then do not allow to the access point to access the network. Deny the permission from the server side.

IV. CONCLUSION

The rogue access point can be easily detected by above proposed system. The proposed system is economic and not more time consuming. The proposed algorithm is more effective for both large scale and small scale local area networks.

REFERENCES

[1] "A Timing-Based Scheme for Rogue AP Detection" - Hao Han, Bo Sheng, Member, IEEE, Chiu C. Tan, Member, IEEE, Qun Li, Member, IEEE, and Sanglu Lu, Member, IEEE.
[2] www.cisco.com/en/US/docs/wireless/wcs/3.2/configuration/guide/wcsmon.html#wp1072373
[3] Air defence, www.airdefence.net, 2009.
[4] Air magnet, www.airmagnet.com, 2011.
[5] Air wave, www.airwave.com, 2011.
[6] L. Ma, A.Y. Teymorian, and X. Cheng, "A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks," Proc. IEEE INFOCOM, 2008.
[7] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, "Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK-Pairs," Proc. Seventh ACM SIGCOMM Conf. Internet Measurement (IMC), 2007.
[8] H. Yin, G. Chen, and J. Wang, "Detecting Protected Layer-3 Rogue APs," Proc. Fourth IEEE Int'l Conf. Broadband Comm., Networks, and Systems (BROADNETS '07), 2007.
[9] S. Shetty, M. Song, and L. Ma, "Rogue Access Point Detection by Analyzing Network Traffic Characteristics," Proc. IEEE Military Comm. Conf. (MILCOM '07), 2007.
[10] H. Han, B. Sheng, C.C. Tan, Q. Li, and S. Lu, "A Measurement Based Rogue AP Detection Scheme," Proc. IEEE INFOCOM, 2009.
[11] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A.Wolman, and B. Zill, "Enhancing the Security of Corporate Wi-Fi Networks Using DAIR," Proc. Fourth Int'l Conf. Mobile Systems, Applications and Services (MobiSys '06), 2006.
[12] "Mobile Systems Location Privacy: "MobiPriv" A Robust K Anonymous System". Leon Stenneth Phillip S. Yu Ouri Wolfsonedu
[13] Aircrack-ng: an 802.11 wep and wpa-psk keys cracking program.
[14] AirDefense Enterprise: a wireless intrusion prevention system.
[15] Wireless Sensor Network Security model using Zero Knowledge Protocol - This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings.