ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

Fake Access Point Detection in Network

Supriya Ayare[1], Sonal Das[2], Varsha Sayanekar[3], parvez siddhique[4], Prof.Raviraj Patkar[5]

Student, Information Technology, Rajendra Mane College of Engineering, And Technology,

Ambav, Ratnagiri, India[1,2,3,4]

Professor, R.M.K.C.E.T, Puduvoyal, Chennai, India[5]

Abstract: Wireless access points are today popularly used for the convenience of internet use. The growing acceptance of wireless local area networks (WLAN) presented different risks of wireless security attacks. The presence of fake access points is one of the most challenging network security concerns for network administrators. fake access points, if undetected, can steal sensitive information on the network. Most of the current solutions to detect fake access points are not automated and are dependent on a specific wireless technology. fake access point is one of the serious threat in wireless local area network. In this paper we have presented our propose solution to detect fake access point &related risk assessment is analyzed .Most of the current approaches to detecting fake access point are rudimentary and easily evaded by hacker. In our solution there is no need of acquire new RF devices for detecting fake access point our solution is designed to work with current infrastructure. Our solution is effective and reliable. It is designed to detect inside attacks in organization.

Keywords: IP & MAC address, fake broadcast packet, WLAN.

I. INTRODUCTION

In today's world the Internet has become essential requirement for everyone, everyone wants to remain connected with the world. Many organizations use Wi-Fi to provide access signals to internet and intranet enabling the flexible workforce. In the field of communications, Banking, industry. The users are most frequently use the internet and information transmitted by the users is broadcasted through the air.Every user within the range of Wi-Fi signal can be easily connect the network and sniffed the information using fake access point.Fake AP is an unauthorized access point plugged into a corporate network, posing a serious security threat.In our project we propose the detection of Fake AP and analyzing related risk assessment.Also provide secure and effective communication.WLAN Security technology has major use in many fields. Wireless LAN has a wid range of applications due to its flexibility and easy access. The use of public Wi-Fi has reached at a level that is difficult to avoid. According to the poll conducted by Kaspersky's global facebook pages 32 percent of the more than 1600 respondents said that they are using public Wi-Fi regardless of the security concerned.

In our proposesolution weconsider IP & MAC address of access point to decide authorised or fake access point.Our solution is effective while detecting fake access point in any organisational network.Thishelp in detecting any security vulnerabilities in network.

II. BACKGROUND

Wireless networking has simplified the network setup and installation time of administrator, but has increased the security threats. Unauthorized access to wireless network is easier than wired network. This access can be for extending the services available on the existing network or to access any confidential information or to tamper the data flowing on the network. One of the simplest techniques is to connect access point in the existing network. As the administrator is unaware of this access point, it is called unauthorized access point or Fake Access Point. Now a days access points are very tiny so physically hiding them is very easy and also they are very cheap.

Right away the cost of wireless networks has dove, and their dependability has significantly enhanced, numerous organizations are joyful to take off wireless Local Area Networks to either develop or supplant their wired systems. The beginning issues in convenience and quality of service (Qos) are no more drawn out basic issues. A large portion of the wireless access points (Aps) and wireless network cards in the business now give up to 54MB or 108MB information transmission speed. Assuming that, the wireless access point of a system is traded off, or exchanged by a malevolent access point, the identity of the legitimate user can effortlessly be traded off. This might permit an attacker to over take the identity of a true blue client and unite with the system as that user, encryption can't ensure against such attacks and accordingly the introductory modest encryption orders for wireless networks have been enlarged with considerably more unpredictable protocols to guarantee that both the system client and the wireless access point could be validated soon after a secure encrypted channel is made.

Wireless networks are growing day by day due to their inherent advantages like less setup time, less maintenance, flexibility so that the network administrator does not have to look after the network problems like wire breakages, connectivity. But the major problem the network administrator has to face in case of wireless network is security. As the medium of communication is air and every communication is broadcast communication, everybody who gets hooked to the network will get access to all the information floating in the network and he can steal the information, misuse the information, corrupt or alter the information.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

Wireless access points are easier to install and the time required to install is also very less. Once access point is installed every one can connect to the network through access point to the existing network and get access to each and every information floating on the network and misuse the information on the network as well. Such access points are called as fake access points and very difficult to detect as they does not provide any identity to the packet floating through them.

III. EXISTING METHODS OF DETECTING FAKE ACCESS POINT

1. IT persons are equipped with wireless packet analyser tool on their handheld device and they will move through the campus for searching access point.
2. Checking the radio frequencies using some sensors placed at different locations in the campus because the access points have property that they broadcast beacon frames containing SSID at regular intervals. So by capturing such frames user can identify presence of access point.
3. Checking the IP traffic on the network. If two back-to-back packet is send on the network then the packets inter-departure time on wireless network is more than wired network.
4. Measuring Round Trip Time (RTT) of the packet send on the network. This is done by sending a packet to the known host (end node) on the network and calculating time when the reply of the packet received. If the round trip time is significantly longer then there exists wireless network.
5. Sending PING fake broadcast request on the network which will be replied only by access points and then determining the rogue access point.

IV. DRAWBACKS OF EXISTING SOLUTIONS

Following are the vulnerabilities of existing some RAP detection tools that need to be removed.

Product Name	Vulnerabilities
Aerohive Hive Manager	Limited reporting, no real time traceing, Very limited documentation.
Ekahau RTLS	Works with only limited number of WLAN system vendors.
Motorola Solutions Air Defence Proximity and Analytics	Available only as an option to WLAN assurance system.
NMAP	Scanning entire network indiscriminately, Intrusive and Noisy, False Positives, Does not Audit Access Points.
AiroPeek	limited by distance, may miss a rogue access point with limited signal range.
Net Surveyor	Not very customizable.
Air Magnet Wi-Fi Analyzer Pro	Works with only limited number of WLAN system vendors.

V. RELATED WORK

The threat of Fake AP have attracted both industrial and academic researchers to work on these problem. There are some methods which focused on this problem. Hao Han and his colleagues used timing based scheme for Fake AP detection, in that they have practical timing based scheme for the user to avoid connecting to Fake AP. In their detection method they have used timing information based on the round trip time. Idea is to user probe a server in local area network and after that measure the RTT(Round-trip delay) from the response, this process is repeated number of times and all RTTs are recorded. If the mean value of RTTs is larger than a fixed threshold, they consider the associated AP as a Fake AP. They have consider four factors that have influence on timing RTT which are Data transmission rate, Location of DNS server, Wireless traffic and APs workload. They have tested accuracy of their technique considering different scenarios for these four factors. Most existing commercial products take the this approach they either manually scan the RF waves using sniffers or automate the process using sensors. Automatic scanning using sensors is less time consuming than manual scanning and provides a continuous vigilance to Fake APs. However, it may require a large number of sensors for good coverage, which leads to a high deployment cost. Furthermore, since it depends on signatures of APs (e.g., MAC address, SSID, etc.), it becomes ineffective when a Fake AP spoofs signatures. Three recent research efforts also use RF sensing to detect Fake APs. In, wireless clients are instrumented to collect information about nearby APs and send the information to a centralized server for Fake AP detection. This approach is not resilient to spoofing. Secondly, it assumes that Fake access points use standard beacon messages in IEEE 802.11 and respond to probes from the clients, which may not hold in practice. Last, all unknown APs (including those in the vicinity networks) are flagged as Fake APs, which may lead to a large number of false positives.

VI. ISSUES ANCHALLENGES

The effects of Fake access points are present on both wired and wireless side of the network. The most of the research work carried out is based on data source from audit trails, system calls and network traffic. In wire network it is very difficult to detect access point by manual audit or placing RF devices to see rang of access point in network. Group is of Industry solutions focusing on wireless only, group is of academic researchers focused on wired side. The Successful wireless-side methods use sensors in the entire network to collect physical-layer and link-layer information to help detect and locate Fake AP in a distributed architecture. Again wireless method is not generally scalable because it includes considerable infrastructural commitment and is costly alternative for huge networks. Beyond that wireless sniffing may failed in certain cases first if Fake AP doesn't show itself by pausing beacon frames, may operate with less signal strength, and may use nonstandard protocols. In the second case sometimes the attacker can even use directional antenna to focus on small area to avoid detection.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

VII. SYSTEM DESIGN

In this section we have explained our problem statement and approach. Our solution is working on any type of network that is wired network, wireless network but only the constraint is all the nodes must be in the same subnet.There are special hardware addresses like in case of broadcast we make all the bits of MAC address one but here we will make all the bits one except first bit which we will keep zero. This is called fake broadcast. As all the bits are not one it is not broadcast address so all the hosts on the network will reject this packet. But we have observed that Access Points are accepting such packets.

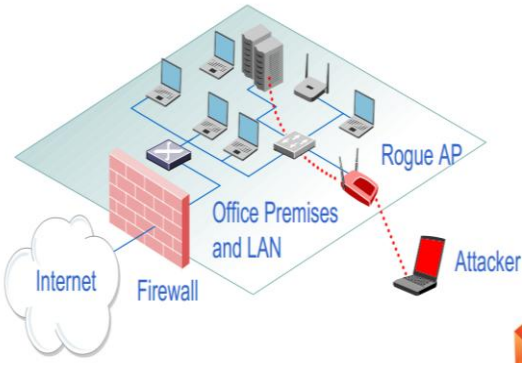

Figure1.Propose solution system

In our propose solution server send a Fake broadcast message to devices present in network. Reply to this broadcast message access point send their IP& MAC address to server in minimum time. Server then compare this IP & MAC address to its database. If that IP & MAC is present in database then that access point is authorised access point otherwise that access point is unauthorised. After getting unauthorised access point in network server send their IP & MAC to client present in their network. To check any unauthorised access point in server network, server send Fake broadcast message after each 30 sec.
Internet Control Messaging Protocol (ICMP) protocol is used for network management and network administration which is working at network layer. We normally use ICMP for ping utility to probe remote hosts for responsiveness. We also have observed that the Access Points are also replying to ICMP packets as well.

For our Proposed System :
Input : fake broadcast packet
Output : IP address, MAC address of the fake AP

Accurate Detection of Fake AP.Consume very less bandwidth of the network. Maintenance cost of our system is also less & our system provides reliable solution to detect fake access point in given network .Solution is secure and scalable.

CONCLUSION

In this paper, we present a fake AP detection method to protect against the stealing of sensitive data in a client-side. Our fake AP detection method measures correlated RSS sequences from nearby APs in order to determine whether the sequences are legitimate or fake. Using the sequential hypothesis testing theory, we predefine the appropriate threshold value Ä using the expected number of iterations. The predefined threshold value enables us to detect fake APs without supervised.

ACKNOWLEDGEMENT

This research was guided by the prof Raviraj Patkar.

REFERENCES

[1] http://blog.kaspersky.com/do-you-use-free-wifi-hotspots-a-survey.
[2] publicWi-Fiusage survey,2012 Identity Theft Resource Centre.
[3] Net stumbler. http://www.netstumbler.com
[4] Wave link, http://www.wavelink.com
[5]The Airwave Project,http://www.airwave.com
[6]W.wei,S.Jaiswal,J.Kuroseand D.Towsley,Identifying 802.11 traffic from passivemeasurments using iterative Bayesian inference in Proc. IEEE INFOCOM 06,2006.
[7]L.Watkins,R.Beyah, and C. Corbett, A passive apporach to rogue access point detection, in Proc. IEEE INFOCOM 06,2006.
[8] Active User-side Evil Twin Access Point Detection Using Statistical Techniques Chao Yang, Yimin Song, and Guofei Gu, Member, IEEE.
[9] A Novel Approach for Rogue Access Point Detection on the Client-Side. Somayeh Nikbakhsh, Azizah But Abdul Manaf, Mazdak Zamani, Maziar Janbeglou
[10] 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.
[11] Online Detection of Fake Access Points using Received Signal Strengths.Taebeom Kim,Haemin Park, Hyunchul Jung, and Heejo Lee