Fake Access Point and Invalid Client Detection and Elimination using Agent Multi Sourcing

Prachi M. Kharat
PG Student
Comp Engg, PVPIT
Savitribai Phule Pune University

N. D. Kale
HOD
Comp Engg, PVPIT
Savitribai Phule Pune University

ABSTRACT
In presently a day's remote (wireless) LAN is broadly utilized as a part of many public open spaces. Wireless access points expand wired network. It gives more flexibility to the clients. One of the fundamental concerns is that of Rogue Access Points (RAP). These security threads which bring about extreme damage to hierarchical information and assets could be because of inside or outer cause. Access point could be one reason which might permit attackers to break the security of authoritative system and permit them to get to sensitive data from system. The access points deployed without clear and definite permission from network administrator are called unauthorized, fake or rogue access point. There are numerous chances of presences of RAP in LAN data.

Rogue Access Points (RAPs) is one of the foremost security threats in current network scenario, if not properly handled in time could lead from slight network faults to serious network failure. Most of the current solutions to detect rogue access points are not automatic and are dependent on a specific wireless technology. In this paper, we propose a Multi-Agent Based Methodology, which not only identifies Rogue Access Point but also completely eliminates it. This Methodology has the following exceptional properties: (1) it doesn't require any specialized hardware; (2) the proposed algorithm detects and totally removes the RAPs from network; (3) it provides a cost-effective solution. The proposed technique can block RAPs as well as eliminate them from the networks both in form of Unauthorized APs or as a Rogue Clients Acting as APs.

Keywords
Rogue Access Point, WLAN

1. INTRODUCTION
To increase range of services of network many organizations have adopted wireless technologies such as WLANs. Due to extensive use of WLANs the performance and security parameters should be considered. There are number of wireless attacks which may severely harm organizational network and security of data. Organization can increase range of its network facilities through access points. Use of access points frees users from being restricted to single location for accessing and using network services and data. By their use user can roam anywhere within range of network and still have access to shared data and resources The resources can be easily accessed and moved from one place to another. It gives more flexibility, portability, mobility to user to have access to resources they require at any place in an organization. But the communication in WLANs is through air so there is risk of third party attacks on user's confidential data. And at the same time communication within peers and internet also have to be maintained continuously. This use of wireless LAN always helps in increasing the productivity of network. The access point is a point which is a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN.

But it is also possible that employees within organization can access unauthorized access point for their personal work and this threatens the security of network. Such access points are called as rogue access points. Many times the user within organization or users with limited resource capabilities are unknown about possible security threats and this breaches the security of WLANS. The attacker may try to masquerade the authorized access point

The proposed system provides a way to detect and eliminate these unauthorized access points in the network by periodic automatic scanning of network. This system does this without use of any specialized device and hence it is cost effective solution to detect and eliminate rogue access points in the network. Whenever the use of layered multi-agent architecture makes system effective, affordable and portable. The master is generated by DHCP enabled network regulates the scanning process of network. During the same period slave agents are generated by master. These slaves dispatch their clones at different clients. When a slave at particular client finds new access point in network it dispatches its clone to that access point along with INFO packet containing MAC address, SSID, channel used etc. details when clone reaches access point it tries to extract the same information from new access point and if the information contained and information extracted is matched then it is a valid access point otherwise it is invalid one and this is reported to master and then that access point is blocked[1].

1.1 Need
Access points installed in company network without explicit authorization from network administrator i.e. rogue access point allows attacker to conduct wireless attacks on company network which may cause severe loss of information to company. To avoid such loss complete, reliable and comprehensive security policies should be implemented. Use of strong and compelling policies reduces the risk of third party users using company resources and information. But there could be a situation where employees within organization may misuse their credentials within company by deploying new access points for their own personal use or for their benefit. This would increase chances of intruder easily getting access to company data and resources.[2] Another case is anyone having access to local network coverage may ignorantly deploy their access points and provide third party user's access to organizational services and data which is serious threat to security of network .In order to avoid such security threat it is required to detect and eliminate such

unauthorized access points.

Use of multiple masters makes system more reliable, autonomous. Conducting automated scan of network does not require users to be trained for its usage. Users can continue their work even during scan is proceeding.[6] This system does not require specialized hardware because of which system is affordable and convenient for use.

1.2 Objective

CMS scheme aims to detect such unauthorized and fake access points and completely eliminates them. It implements a fully automated approach which reduces human efforts and saves user's time.

1.3 Theme

In current scenario there is extensive need to share network services and resources, since users are located at different sites due to which wireless access to network services has increased to a great extent. Some eminent properties of WLANs such as flexibility, ease of access, affordability and ease of use etc. have increased rate of wireless LANs being deployed and used in many corporate and academic research areas. In order to increase range of their services many organizations use access points. But as there is increase in use of wireless systems, maintaining network security and data integrity, Confidentiality are primary worries. These security threats which may cause severe harm to organizational data and resources could be due to internal or external causes. Access points could be one of the reasons which may allow attackers to breach the security of organizational network and allow them to access sensitive information from network. Access points allow users to roam anywhere in company area and still have access to network data and facilities. To deploy new access point prior authorization from network administrator is necessary. The access points deployed without clear and definite permission from network administrator are called unauthorized, fake or rogue access point. There are many chances of presence of rogue access point in wireless LAN since attacker does not require very detailed knowledge or expensive devices to deploy such fake access point. By use of such access points third party person can easily gain access to network facilities and confidential data.

2. LITERATURE SURVEY

Before developing the tool it is necessary to determine the time factor, and number of the people working for that work. Once these things are satisfied, then next step is to decide which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of peripheral support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

2.1 Current Wireless Network scenario

In current wireless network scenario intruder may deploy their access points within wireless LAN area which would provide strong signal for providing network services as compared to authorized access point in network because of which wireless client would prefer such access points more as compared to authorized one. This is a point where chances of wireless attacks increase to a great extent .In such circumstances organizations should be able to cope with security threats. Figure below describes the current wireless network scenario.

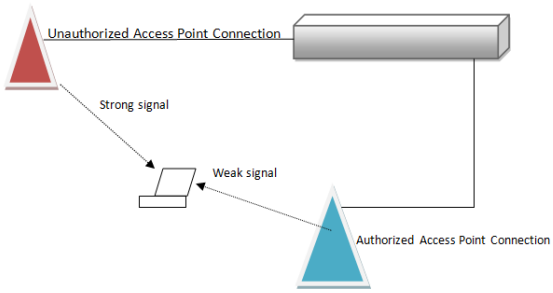

Fig 1. Wireless network scenario

2.2 Current approaches

In current wireless scenario there are basic two approaches which are currently being implemented to detect rogue access points. The basic network scenario is divided into two categories:

1. Wired approach
2. Wireless approach

In wired approach use an existing wired LAN to scan and detect access points. Such method includes TCP fingerprinting, SNMP scanning, sniffing.

2.2.1 TCP Fingerprinting

In this method, various specially crafted packets are used to examine the behavior of how particular target responds .This can be determined observing the changes in response probe sent by target system. Advantages of TCP fingerprinting are that once we start scan user don't have to intervent during scan to observe the result. Where disadvantage of this method are is that it could take long time to scan if network is large. Another disadvantage is this method is not 100% accurate.

2.2.2 SNMP Scanning

SNMP fingerprinting is similar to TCP fingerprinting but instead of using information of TCP/IP stack it uses information obtained by SNMP protocol. An advantage of this method is you can start scan and can continue to do other things. The disadvantage of this approach is that not all APs support SNMP and it may turn off which makes it impossible to get information on device.

2.2.3 Packet Sniffing

In this method a device is configured to run in promiscuous mode and analyze packets and examine Ethernet headers to check that MAC addresses are authorized addresses. Advantages of this method are it is a continuous process and constantly monitors unauthorized MAC addresses.
Disadvantages are problem of scalability, if network is high speed network then it would be difficult to analyse all traffic and monitor invalid MAC addresses
Similarly, wireless approach is further categorized into following categories:

2.2.4 Active Probing

This method uses probe request frame on each channel to determine suspicious wireless activity. When an access point comes within the range of the client and receives a probe request frame it will typically reply with a probe response frame containing the network ESSID. Advantage of using this method is that it is the easiest method to implement. But at the same time the person to detect rogue access point must walk around the building with laptop or handheld device which is time consuming and expensive. Periodic walk through the

campus is the only way to detect unauthorized access points in network.

2.2.5 RF MONITORING

This method has a client with wireless card configured in radio frequency mode that can capture all RF signals on all channels. This method can detect rogue access point by monitoring raw 802.11 frames to detect if there are any telltale frames broadcast by rogue access points.

One disadvantage of RF monitoring to work the client must be in the range of access point. Another disadvantage is that it has limited support since it works only on linux and BSD based applications.

2.3 Tools used for Detection of Rogue access points

There are many tools which help organization in finding or detecting presence of rogue access point in wireless network.

2.3.1 NetStumbler

This tool helps user find the WLAN areas suffering from weak signal. Issues related to areas suffering from weak signal and presence of rogue access point can be easily found by using this tool. Network interference can be easily detected using this tool[12].

2.3.2 Airsnare

It is a program for windows that detects presence of device with unauthorised MAC address or DHCP requests. In case of unauthorised MAC address an intrusion alert is sent to the administrator to notify presence of malicious device[14].

2.3.3 AirMagnet

Air Magnet uses access control lists (ACLs) and scans continuously from each sensor for rogue or unknown devices. Rogues are automatically found, located, optionally triangulated, optionally blocked on the wire and wirelessly, and the system notified designated people or other systems[13].

2.3.4 Kismet

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plug-ins which allows sniffing other media such as DECT. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of non beaconing networks via data traffic.[17]

Since use of insecure access point threatens the security of not only its owner but also to the security of all users who access it. A single master agent system discussed in [1] uses an approach where there is a single master agent which later may prove to be insecure as the number of clients' increase there are chances of system overload due to which the single master agent may fail. In [2] unauthorized access points are detected based on accuracy of clock skew which determines spoofing of MAC address. Main goal is to determine consistency of clock skew throughout the process of scanning network and differentiating packets sent from fake and authorized access points.[3] Gives classification of various access points and also describes the design using distributed monitoring module framework. Authors of [4] have proposed a system with intrusion detection system that detects rogue access points along with generation of X.509 certificate and use of VPN solutions that eliminates shortcomings of WEP.[5] Describes approach to secure data using frame collectors and mobile agents to detect rogue access devices in wired and wireless environment. Authors of [6] proposed an approach to detect rogue access points in distributed environment using mobile agents. [7] Describes a passive approach to detect rouge access points using RTT to distinguish wired and wireless traffic independent of WLAN standards such as 802.11a/b/g. Authors of [8] proposed an approach of analyzing traffic characteristics of WLAN patterns and show that wireless links are more limited of spreading packets as compared to wired links but this is based on all impractical assumptions such as wired and wireless links are connected gateway, router or at most two links and so on.[9] Implements an approach to secure WLANs using an security architecture of mobile agents which allows users to freely choose variety of encryption techniques and secure their information[18].

3. PROBLEM STATEMENT

To utilize the company services and increase degree of resource and information sharing WLANs are being adopted excessively by many organizations. In these WLANs medium of information exchange is through radio frequency waves in air. So all nodes within network can communicate through air. Because of use of wireless technology there are chances of unauthorized users trying to get access to organizational sensitive information and utilize network resources and services free of cost. To extend range of services of network organizations make use of access points. Third party users may try to have control over these access points by masquerading the authorized access point in network. So that it appears to be authorized access point and easily get access to information and shared resources. Such access points can be deployed by employees within organization for their personal benefit. In order to cope with this problem there is need to detect and eliminate such unauthorized access points.

4. PROPOSED SYSTEM

The agent multi sourcing scheme overcomes above issue by using automated system that scans entire network and lists available access points in network. There are two levels of mobile agents which regulates the work of determining fake access points. In proposed system a multi-agent based methodology is used which not only detects rogue access points but also eliminate them completely. The proposed algorithm detects and eliminates unauthorized access point without human intervention between scans. No extra cost is to be paid for specialized hardware or software. This gives a cost effective solution to cope up with wireless network security threats.

4.1 Defining Requirements for New System Statement of Scope

The CMS scheme is developed on java which makes use of scanner class which is an in built utility that consists of different methods by using which we can scan network. This system requires the list of registered access points which is maintained at DHCP server. Master agent works as central repository and it is responsible for regulating authentication process of wireless access points. To operate this system does not require explicit training to employees working on it. The INFO packet containing crucial information about any valid access point is encrypted to prevent it from being spoofed. System provides autonomous and fault tolerance through use of mobile agents[4].

4.1.1 Initial Condition

Following are some initial conditions to be considered:

1 Application must be installed and DHCP server must be turned on before operating the system

2 Wireless LAN devices should be in range and registered with DHCP server.

3 All devices must be configured with 802.11 a/b/g standards.

4.1.2 Major Input to the System

1. Initial input to system is the range of IP addresses from which it should start scanning network devices. Along with this initially it searches for hostname, status, MAC address, IP address etc. of each access point in range of WLAN and puts them in a list.

2. After getting list of these access points the IP addresses are checked for within range or not.

4.1.3 Output from the System

The outcomes of system is list of valid and invalid access points along with their details such as MAC address, IP address, channel, SSID and status which determines whether access point is permitted or connected and if it is invalid its status is set to blocked and shown in the list of access points.

Software Context

The proposed system is expected to detect presence of unauthorized access points in WLAN through use of mobile agents. These mobile agents should migrate to access point and extract the INFO packet to determine validity of access points in network. After determining its validity if it unauthorized access point then master agent should block it otherwise if it is a valid one then access point should be allowed to get connected to network[4].

Major Constrain

System must be equipped with 802.11 standards and should have DHCP enabled network so that during scanning initial process we get the list of registered access points and it will be easier to determine validity of access points in network.

Outcomes

Invalid Access points are identified and blocked.

5. SYSTEM ARCHITECTURE

Fig. 5.1 gives abstract view of proposed system. This system architecture represents different system components involved.

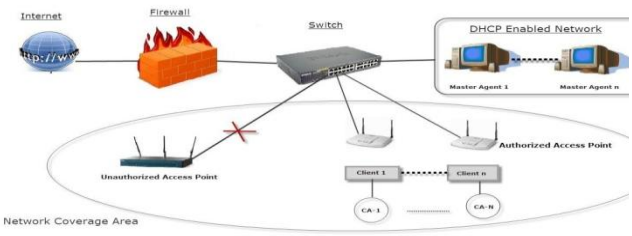

Fig.2. System Architecture

The architecture mainly contains the network setup with access points and DHCP-M server. If currently working master agent fails due to physical damage or power failure then another master agent is automatically generated. This master agent is responsible for creating & dispatching slaves at each access point. These slaves are again cloned and sent to the client side. Whenever this cloned slave finds presence of new access point in network it automatically creates and sends INFO packet to new access point which validates the entry of AP or client into network. The DHCP server will act as a central repository for network.

5.1 Advantages of System

5.1.1 Reduction in Network Load

Mobile agents are dispatched to the remote hosts containing the data. The agents perform the computations at the remote hosts and return back with the results. Since computations are moved to the data storage location instead of moving data to the computing location, network load is reduced[3].

5.1.2 Overcome Network Latency

Mobile agents can be directly dispatched from the central controller in setup to the APs & client side. The agents act locally and directly execute the controller's directions.

5.1.3 Asynchronous and Autonomous Execution

Mobile agents operate asynchronously. Once a mobile agent is dispatched from the central server machine, the server machine can disconnect from the network. The mobile agent executes autonomously without the intervention of the server machine. The server machine can reconnect at a later time and collect the agent.

5.1.4 Fault Tolerance

In the system the agents are communicating together since their behavior is autonomous to the environmental changes and they react dynamically to the changes hence if server is going to shut down it will be informed to agents and accordingly they will react to changes. This makes system fault tolerant in case of network failures.

5.2 Algorithmic Steps

a. Generate Master agent at DHCP Sever.

b. Generate Slave Agents at master agent depending on number of access points in network.

c. Dispatch slave agents to all access points.

d. Clone slave agents created at all access points.

e. Check presence of new access point in the network by client, clone agent at client side and automatically build INFO packet and send it to related slave agent.

f. Slave agent forwards it to Master Agent.

g. If information in INFO packet is matched, then new slave agent generated for that new access point by Master Agent, else it is detected as fake access point.

h. If information does not match, then steps given below are taken to block that fake access point.

i. Extract the MAC address from INFO packet.

j. Extract the network switch address based on that extract MAC address.

k. Extract the connected port number based on MAC and Switch address.

l. Finally block that port number from any other wireless LAN traffic.

6. ACKNOWLEDGMENTS

I take this golden opportunity to owe our deep sense of gratitude to my project guide Prof. N. D. Kale for her instinct help and valuable guidance with a lot of encouragement throughout this paper work, right from selection of topic work upto its completion. My sincere thanks to Head of the Department of Computer Engineering Prof. N.D.Kale and Prof. Y.B. Gurav who continuously motivated and guided us for completion of this paper. I am also thankful to our PG Coordinator, all teaching and nonteaching staff members, for their valuable suggestions and valuable co-operation for partially completion of this work. I specially thank to those who helped us directly-indirectly in completion of this work successfully.

7. CONCLUSION

Detection and elimination of rogue access points is done using multiple master agents which has made system 50% more flexible than single master agent and easy to use. As multiple masters are used the system architecture is made 80% more faults tolerant than single master agents system. It continuously and automatically scans network by specifying IP range so need not to scan network manually and does not require explicit configuration of each access point with master, it automatically scans and lists all available access points. It works on any wired or wireless network connection to detect and eliminate rogue access points. In this system if one master fails another will handle the requests so load balancing is achieved. As no specific devices are required so cost compared to other tools is 20 to 30% less. In this system we can scale the performance by actually viewing rogue access points found and blocked and as strong GUI is provided system is very easy to use.

There is no use for the blocked port, in future scope we have to try something to do for that blocked port, it must use in future and utilize that port for other purposes.

8. REFERENCES

[1] Prof. Sandeep Vanjale, Dr. P.B.Mane, "A Novel approach for Elimination of Rogue Access Point in Wireless Network",IEEE,2014.

[2] Hao Han, Fengyuan Xu, Chiu C. Tan,Yifan Zhang, and Qun Li, "VR-Defender: Self-Defense Against Vehicular Rogue APs for Drive-Thru Internet", IEEE trans. , Vol. 63, No. 8,October 2014.

[3] Liran Ma,AminY. Teymorian, Xiuzhen Cheng *"A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks"*publishedin the IEEE INFOCOM 2008

[4] M. K. Nivangune, Prof. S. B. Vanjale, Dr. P. B. Mane,"Detecting Unauthorized Access Point in WLAN by using CTT", IJARCSSE, vol 5, Issue 7, July 2015.

[5] Mrs. Fatima D. Mulla, Mr. Sandeep Vanjale, Prof. Dr. P. B. *Mane " PROVIDING DATA SECURITY FOR WI-FI NETWORK USING MOBILE AGENT IN DISTRIBUTED SYSTEM"* International Journalof Advanced Engineering Technology E-ISSN 0976-3945 IJAET/Vol.III/ Issue II/April-June, 2012/127-130 Research Article.

[6] Prof. Suryawanshi Govind R,Prof. S.B.Vanjale *"Architecture of mobile agent for Distributed rogue access point detection in distributed system"* CSCIT,Nanded on09Jan2010.

[7] MohanK Chirumamilla,Byrav Ramamurthy*"Agent Based Intrusion Detection and Response System for Wireless LANs"*CSE

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

[9] Songrit Srilasak,, Kitti Wongthavarawat and Anan Phonphoem, Intelligent Wireless Network Group(IWING) *"Integrated Wireless Rogue Access Point Detection and Counterattack System"*publishedin2008 International Conference on Information Security andAssurance.

[10] V.S. Shankar Sriram,G. Sahoo *"A Mobile Agent Based Architecture for Securing WLANs"* International Journal of RecentTrendsinEngineering, Vol 1, No. 1, May2009

[11] MS. Snehal Behede,S.B.Vanjale,P.B.Mane*"Provoding data security in WLAN by detecting unauthorized access points and attacks"*Intenational JournalOf Engineering Science And Technology.

[12] NetStumbler- http://www.netstumbler.com

[13] AirMagnet-http://www.airmagnet.com

[14] http://www.softpedia.com/get/Network-Tools/Network-Monitoring/NetStumbler.shtml

[15] http://www.leger.ca/pages/CHAMPLAIN/WLAN-tools.htm

[16] www.ias.ac.in/resonance/July2002/pdf/July2002p35-43.pdf

[17] http://www.kismetwireless.net