Evidence Tracking For Rouge Access Points (RAP) Detection Using Mobile Agent

Ms. V. V. Nikam[1] , Prof. S. K. Sonkar[2].

Student of Master of Computer Engineering, AVCOE, Sangamner, Ahmednagar, Maharashtra, India[1]
Asst. Professor in Computer Engineering Department, AVCOE, Sangamner, Ahmednagar, Maharashtra, India[2]

ABSTRACT: **Now a day's out of number of security problems in current networks scenario, Rouge Access Point is the major security problem. As such no satisfactory solution had identified though a lot work has been done on RAP. They are dependent on the specific wireless technology. In this paper, we propose the integrated solution for detection and eliminate rouge access points. This methodology has following properties: 1. it doesn't require any specialized hardware; 2. the proposed algorithm detect and eliminates the RAPs from network; Our proposed solution is effective and low cost.**

***Keywords*— Rogue Access Point, Wireless Security, Hybrid LANs, Mobile Agent.**

1.INTRODUCTION

Wireless networks are common everywhere from coffee shops, corporate offices, research labs and city parks. of For ease of consumption these networks are commonly implemented and where cable is not an option their capability to provide network access to areas . Wireless networks allow users to provide guests with internet access. Due to the ease of access and also mobility, the attacker can attack as malicious easily from the most unexpected locations. As Wireless networks does not possess any defined borders, air waves can be penetrated into unintended areas, which allows the attacks from the malicious attackers to bypass perimeter firewalls, sniff sensitive information and access the internal network, attack wireless hosts without direct access to the network.Presently lot of organizations uses the wireless LAN to provide the access channel to the Internet and Intranet enabling the flexible workforce. Employees are the liberty of mobility along with their workstations i.e computers from one location to another with maintaining the communications with peers and with precaution that the Internet connection to be continuously maintained, Ultimately It shows that utilizing wireless LAN helps to increase the productivity of a company.

Still today wireless security is always a primary concern. As Air is the medium for transmission of the information by the users, and anyone within range of the wireless signal have the easy access to tune in and capture the data. Many enterprises while going to wireless communication include the wireless security measure such as IEEE 802.11i or WPA (Wireless Protected Access).IEEE 802.11i provides the encryption and authentication mechanisms to protect user from unauthorized access and data eavesdrop over the wireless network. However, such security measures cannot protect the system from their own staff to restrict the unauthorized installation of the access point. The staffs can easily plug in the unauthorized access point (normally called rogue access point) to the network for their personal usage due to the unawareness of the staff and which gives security threats that come along with this act. And the resultant for this is, the hacker can bypass the company's line of network defences (i.e., firewall, access control) through the rogue access point and produce the serious threat to the organization.

The Rogue Access Point is known as an unauthorized AP in the literature. Wireless access point installed on a secure network without proper authorization from a local administrator, which allow a cracker to conduct a man-in –the middle attack or can be used by adversaries for committing espionage and launching attacks. According to an early study by Gartner, Rogue APs are available near to 20% of all enterprise networks.

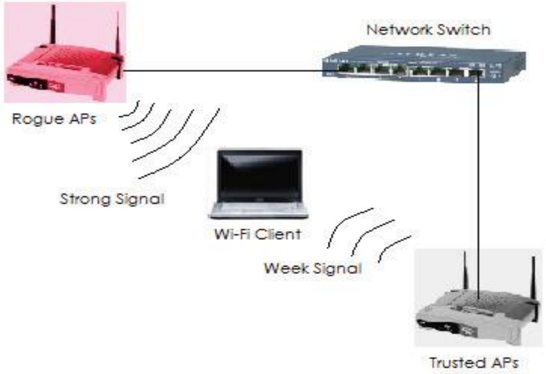


Fig.1 RAPs Higher Broadcast Power than Normal APs.

Most of the time “Rogue” APs are being installed by the user to increase the range of the network but without proper authorization, which results in a security hole which may be exploited by intruders, or intruder himself planting an AP with a higher broadcast power than normal to masquerade as a legitimate AP[Fig -1].

This paper proposes an architecture showing the use of mobile agents to achieve security in WLANs. Our architecture gives a secured means of key generation and key distribution opening the avenue for WLAN users to choose an encryption technique of his choice. The purpose of this information is to study or evaluate current WLAN technologies with regards to security and current solutions against wireless attacks. security and current solutions against wireless attacks.

2.EXISTING SYSTEM

A good or quite research and work has been carried out for the efficient ways for detecting rogue access point in wireless LAN, still this is grey spot area where we have good opportunity for further investigation in this line as no such satisfactory level solutions derived, which is far enough. The brief data of the same has been stated below.

A. Related Work

There are two broad classes for detecting RAPs viz. i. Monitoring RF waves, ii. Monitoring IP traffic. Many existing commercial products shows approach by either manually scanning of the RF waves using sniffers or atomisation the process using sensors. Three recent study research efforts uses RF sensing to detect rogue, wireless clients are configured for collecting the information about nearby APs and sending the information to the centralized server for RAP detection. The intension of system is to give the dense RF monitoring through wireless devices which are attached to desktop machines. The purpose behind this is to detect the protected layer- 3 RAPs. The study is of RAP detection by monitoring IP traffic. The authors with demonstrated experiments in a local tests that with wired or wireless connections can be separated by visually inspections at the timing in the packet traces of traffic generated by the clients. The technique is to segment large packets into smaller one.

B. Demerits of existing works

1- Manual 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- Methods to be required in mobile computing should be with less power consumption. But 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 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.

3. SYSTEM ARCHITECTURE

The main purpose of the project is for the design an interface for detection of intrusion in wireless LAN. We will be designing server model for managing WLAN, which keeps track of every client, also fetch data from remote place, save it in database.

A. Mobile Agent Architecture

The scheme is designed for its independency on any operating system or system auditing implementation. Figure 2 shows the approach taken. The agent captures each audit record produced by the native audit collection system. A filter is applied but it retains the records only those are of security interest. Those are changed into a standardized format which referred to as the host audit record (HAR). A template-driven logic module analyzes the records for suspicious activity. At the lowest level, the agent scans for events that are of interest independent of any past events. Like which include failed file access, access of system files, and change the file's access control. In the next higher level, the agent provide the sequence of events, such as known attack patterns (viz.signatures). Lastly, the agent take a look for anomalous behaviour of an individual user based on a historical profile of the user, for example number of programs executed, number of files accessed.

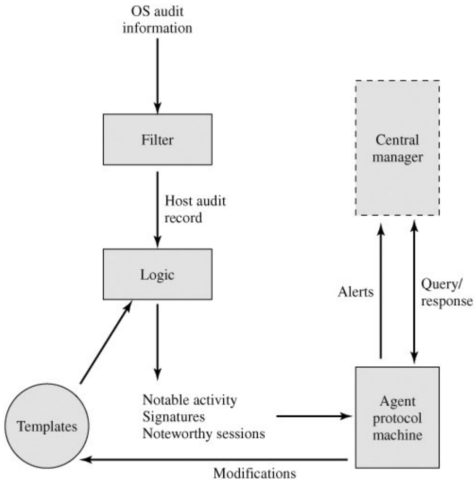


Fig 2. Mobile Agent Architecture

Whenever the suspicious activities are detected, alerts are sent to the central manager. The central manager give an indication to an expert system that can draw inferences from received data. The manager may also ask individual systems for copies of HARs to correlate with others. The LAN monitor agent gives the information to the central manager. LAN monitor agent does the audit for the host-host connections, services used, and volume of traffic. It searches for prominent events, like sudden changes in network load, the use of security-related services, and network activities for example login.

Mobile agents are nothing but computer programs, which may be autonomous, proactive and reactive, and have the ability to learn. There is the movement from one node to another node and interact with each other, sharing information to better carry out goals. Mobile agents spread intelligence across the network, while moving in a network. The mobility of mobile agents allows them to be created, deployed, and terminated without disrupting the network configuration.

Mobile agents are computer programs, which are autonomous, proactive and reactive. They move from one node to another node and interact with each other, sharing information to better carry out their goals. While moving in network, Mobile agents spread intelligence across the network. The mobility of mobile agents, gives them to be created, deployed, and terminated without disrupting the network configuration. Mobile agents programs being sent across the network from the client to the server or vice versa. An agent that can be executed after being transferred over the network will be called an agent host. A software agent is a common name and describes a software entity that computerizes some of the difficult tasks on behalf of human or other agents.

The remote programming using mobile agents is considered as an alternative to the traditional client-server programming based on the remote procedure (e.g. CORBA).A software agent is known by a life-cycle model, a computational model, a security model, and a communication model. But a mobile agent is also identified by a basic agent model and navigation model.

After initial era of mobile agent, the current expectations of research community from mobile agent are more demanding and realistic. With one after decade of first of mobile agents, it is now clear that mobile are best suited for remote information retrieval. With the Consideration of nature of mobile computing , the use of mobile agent become unavoidable where computing hosts are away from each other and in such scenario if we want to know what is happening on remote host,. Hence the detection of presence of RAP in wired, wireless or hybrid type of network is a fit case for use of mobile agent for such detection

B. Architecture of Rogue access point detection using mobile agent

Abbreviations used :

SA- Server Application

MAS- Mobile Agent System

MA- Mobile Agent

Proposed mobile agent based architecture for rogue access point detection.

C. Experimental Set-up

As shown in figure 3, consider a hybrid network (wired + wireless). Wired network is recognized with the help of layer-2 switch. Authorized AP is connected this layer-2 switch. We will expand client-server software where server application(SA) will keep generating sufficient long alpha numeric string after every one minute and will broadcast this string over entire network(wired as well as wireless). Here in this architecture we will organize Server Application on server. Client Application will be deployed on each authorized client in the network. Client Application will send acknowledgement to Server Application, every time it receives alpha-numeric key from Server Application. Client Application when receives key from Server Application, stores it in text file on client on which it is deployed. Mobile Agent System will be deployed on all authorized client in network. As and when new client will come in network, system administrator is supposed to deploy Client Application and Mobile Agent System on these new clients. Only after such deployment these new clients will be allowed to operate in network. As shown in figure 1 in case-I attacker installs RAP either in NIC (Network Interface Card) port or in switch port. Our target is to detect this rogue access point. Behind this rogue access point there will be unauthorized client i.e client 7. This client 7 will not have Mobile Agent System and Client Application installed on it.

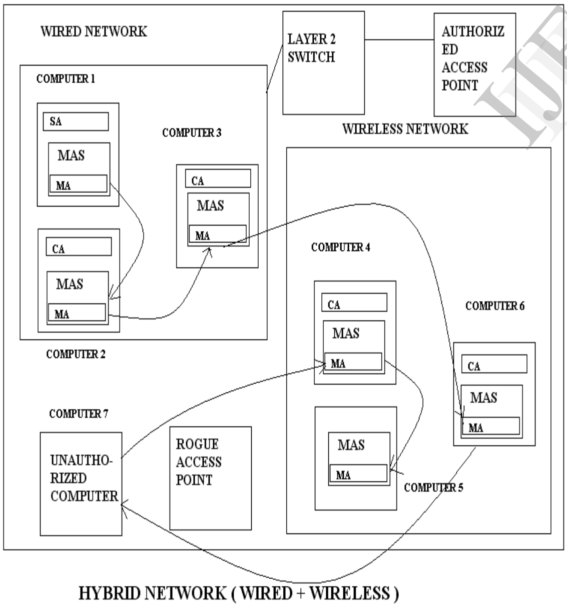


Fig.3 Mobile agent based architecture for rogue access point detection

C. Detection Methodology

At the start, alpha-numeric strings will be generated by SA after every one minutes and afterwards will broadcast the key over entire network. Clients which will be active at that time will trace these key strings and will acknowledge them. Same time Mobile Agent will start from server. Server Application will itself save generated alpha-numeric strings in file. Mobile Agent will take this file from Server Application. MA will randomly select any lively client from network and will visit that client. Say client 2 as shown in figure 1. After reaching there Mobile Agent will ask client 2 to give any past created alpha-numeric string. This selection of past-generated key, may be asked, alpha-numeric key which will be purely random in manner so that attacker will find it complicated in guessing the pattern of alpha numeric string. As client 2 is an authorized computer, it will have that alpha-numeric string with it and client 2 will generate it and will get authenticated. After this Mobile Agent will beginning for another new client by using random client selection method. Say client 3 as shown in figure 1. Just like client 2, as client 3 is also certified computer it will also get authenticated by Mobile Agent. After this Mobile Agent will again run random algorithm and will select next client to visit. Say client 6. Client 6 will also get authenticated as it is also certified client. After this let us suppose Mobile Agent tries to visit client 7 which is unauthorized client. As client 7 will not have Mobile Agent System and Client Application deployed on it, Mobile Agent will not get executed on client 7. As Mobile Agent is not getting executed on one of client of your network, this will be measured as serious crime and access point connected that client will be declared as rogue access point. In this way we managed to detect RAP. After visiting all computers Mobile Agent will return to server and will take newly updated file of alpha-numeric key from Server Application. After that it will again keep visiting clients in network in above mentioned manner.

4.MATHEMATICAL MODULE

Set theory:- A set is defined as a collection of distinct objects of same type on class of objects. The object of a set are called elements or members of the set. Object can be number, alphabet, names etc

Mobile Agent:
Set(M)={O,1,2,3,4,5,6,7,8,9}
0= Spawn N thread as the number of clients in the cell.

1= Fetch Audit information from the client Machine
2= Send audit information to Server.
3=Save alphanumeric key at client side
4=Compare alphanumeric keys at server and client side
5=If comparison is true set flag=1.
6= Notify central administrator for IDS Detection alert.
7= Request Blocking that Client
8=Otherwise, set flag=0
9=Save next alphanumeric key at client side

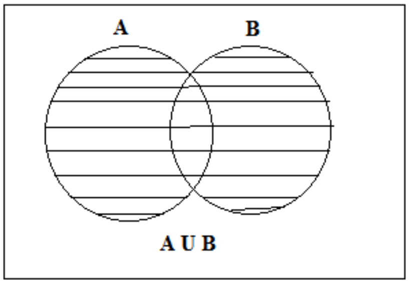
Sever Application:
Set(S)={1O,11,5,12,13,8,14,15,16,17,18}

10=Upload mobile agent
11= Wait for notification of possible IDS alert from agents of cells
12= Search for corresponding IP Address from database.
13= Inform that the system is attacked to administrator.
14=As per the request of admin Block the client
15=Perform scanning of network
16=Add information of client after every one minute to the database.
17=Generate a alphanumeric key after every one minute
18=Broadcast same key to network using MA

Mobile Agent System:
Set(P)={19,10,3,20}
19=Upload mobile agent system on client
20=Show alphanumeric string to Mobile agent

Set(M)={O,1,2,3,4,5,6,7,8,9}
Set(S)={1O,11,5,12,13,8,14,15,16,17,18}
Set(P)={19,11,3,20}

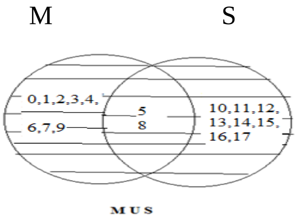
Union of sets:-
Union of two sets A & B is defined to be the set of all those elements which belongs to set A or set B or both and is denoted by A U B



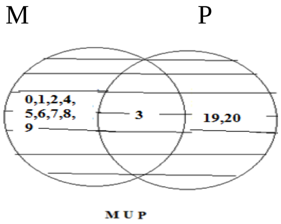
In our project we are drawing the mathematical module and showing the union operation on different sets. They are as follows

1) M U S
2) M U P
3) S U P

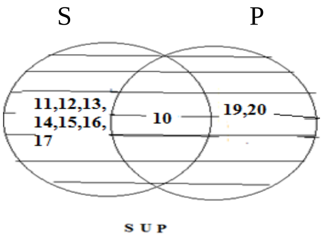
1)MUS={0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18



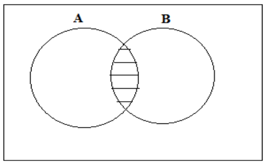
2) M U P = { 0,1,2,3,4,5,6,7,8,9,19,20}



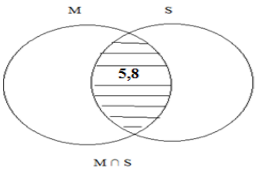
3) S U P = { 1O,11,12,13,14,15,16,17,18,19,20}



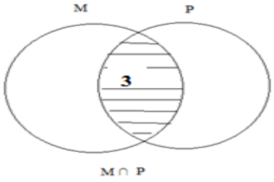
Intersection of sets:-
Intersection of two sets A & B is defined to be the set of all those elements which belongs to set A and set B



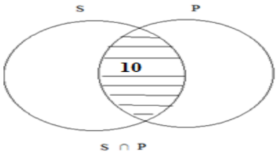
5) M ∩ S = {5,8 }



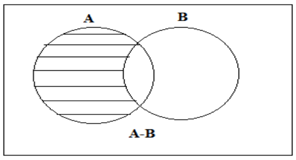
6) M ∩ P = {3}



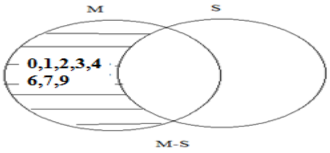
7) S ∩ P= {10}



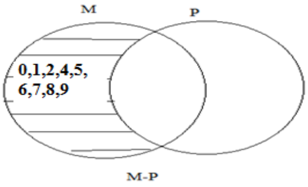
Difference of sets:-Union of two sets A & B is defined to be the set of all those elements which belongs to set A but do not belong to set B and is denoted by A.



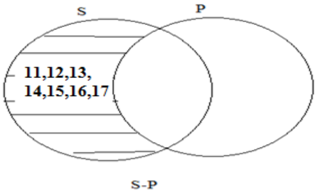
9) M-S={0,1,2,3,4,6,7,9 }



10) M - P ={0,1,2,4,5,6,7,8,9}



11) S-P={11,12,13,14,15,16,17}



5.OBJECTIVE

The software that we develop should be capable of

1- It does not use any signature checking, it is free from spoofing attacks.

2- Can be used in Hybrid network i.e. wired, wireless or both.

3- Because of increase in processing power of client, transparency generated by Mobile Agent will much less.

4- With progress in time, text file will have more entries resulting into stronger authentication.

5- Can detect layer-2 as well as layer-3 access points.

6- Will generate less false alarms.

7- Mobile agents add fault-tolerance. The network is not defenceless to a single-point of failure.

8- It is extremely difficult for an intruder to disrupt working of mobile agent based system.

9- Mobile agents can take advantage of the inherent parallelism of large networks to offer performance improvements over conventional centralized security monitoring by distributing the workload over the network.

10- Distributed rogue access detection using mobile agent scales well as more agents clones can be added when new clients are added to the network. Maintaining and upgrading the mobile agent based system can be accomplished by dispatching or cloning new agents and retracting or disposing of old agents.

11- Agents can be adaptively assigned to different tasks spanning a range of responsibilities from intrusion detection and diagnosis, to reconfiguration and recovery.

12- Agents can be developed to run on heterogeneous computer systems and take advantage of the built-in agent communication capabilities.

6. Expected Result

We are try to give best result than previous results..As it does not use any signature checking, it is free from spoofing attacks. Can be used in any type LAN i.e. wired, wireless or both. Because of increase in processing power of client, overhead generated by MA will much less. With progress in time, database file will have more entries resulting into stronger authentication. Detection is protocol neutral Can detect layer-2 as well as layer-3 access points. Mobile agents add fault-tolerance. The network is not vulnerable to a single-point of failure. It is extremely difficult for an intruder to disrupt working of mobile agent based system.

7.CONCLUSION

In this project we have proposed architecture for detecting rogue access point in IEEE 802.11 networks using mobile agent. Our method overcomes various drawbacks of existing methods available for said purpose. Further research on issues like after how many minutes alpha-numeric strings can be generated, total number of mobile agents to be used, strengthening string generation etc. can be done.

Advantages of Architecture:

- As it does not use any signature checking, it is free from spoofing attacks.
- Can be used in any type LAN i.e. wired, wireless or both.
- Because of increase in processing power of client, overhead generated by MA will much less.
- With progress in time, database file will have more entries resulting into stronger authentication.
- Detection is protocol neutral
- Can detect layer-2 as well as layer-3 access points.
- Will generate less false alarms.
- Mobile agents add fault-tolerance. The network is not vulnerable to a single-point of failure.

It is extremely difficult for an intruder to disrupt working of mobile agent based system.

REFERENCES

[1] V. S. Shankar Sriram, G. Sahoo, Krishana Kant Agrawal "Detecting and eliminating Rouge access Points in IEEE 802.11 WLAN – A Multi-Agent Sourcing Methodology" 2010 IEEE 2nd International Advance Computing Conference.

[2] V. S. Shankar Sriram, G. Sahoo "A Mobile Agent Based Architecture for Securing WLANs" International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009

[3] Mohan K Chirumamilla, Byrav Ramamurthy "Agent Based Intrusion Detection and Response System for Wireless LANs" 0-7803-7802- 4/03/$17.00 © 2003 IEEE

[4] Songrit Srilasak,, Kitti Wongthavarawat 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.

[5] Liran Ma, Amin Y. Teymorian, Xiuzhen Cheng "A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks" published in *the* IEEE INFOCOM 2008

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

[7] Songrit Srilasak, Kitti Wongthavarawat, Anan Phonphoem "Integrated Wireless Rogue Access Point Detection and Counterattack System" 2008 International Conference on Information Security and Assurance

[8] "Rogue Access Point Detection" Automatically Detect and Manage Wireless Threats to Your Network-www.wavelink.com.

[9] White Paper: Access Point Detection via Crowd sourcing.

[10]Distributed rogue access point detection in wireless IEEE 802.11using Mobile Agent by Dhaygude A.V.,.Karyakarte M.S,.S.B.Vanjale, Prof.Mrs.M.S.Vanjale

[11]" 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.

[12] AirMagnet. http://www.airmagnet.com.

[13] NetStumbler. http://www.netstumbler.com.

[14] AirDefense, Wireless LAN Security. http://airdefense.net.

[15] Rogue Access Point Detection: Automatically Detect and Manage Wireless Threats to Your Network.

[16]http://www.proxim.com.