Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Rouge Access Point Detection and Elimination using Mobile Agent Methodology

Ms. Nikam Vidya V*, Prof.S.K.Sonkar, Prof.Suryawanshi G.R
Computer Engineering,Pune University
Pune, India

Abstract—Now day's Networks are foundation for dissimilar types of security problems. Rouge Access Points is one of the major security problem in present network circumstances. Many of work have been made in recognition of intruders. Lot of solutions are distant from satisfactory. All solutions are dependent on the specific device or wireless technology. In this paper, we propose the incorporated solution for detection and eliminate rouge access points (RAP). This method has some properties like it doesn't need any particular hardware and the future algorithm detects and eliminates the RAPs from network. Our proposed solution is low cost and very efficient.

Keywords—Rogue Access Point, Wireless Security, Wireless LANs, Mobile Agent, Intrusion detection system.

I. INTRODUCTION

The increasing importance of network security is variable security concerns towards the network itself rather than being host based. Distributed Approaches to agreement with varied open platform and support scalable result and security services must be surfacing into network-based. (Intrusion Detection System)IDS must evaluate and associate a large volume of data together from different serious network access points. The intrusion detection technology is the method of identifying network activity which can be lead to a negotiation of security policy. This task requires an IDS to be able to distinguish distributed patterns and to detect situations where a sequence of intrusion events occurs in multiple hosts. Computer networks are always showing too many kinds of cybercrimes when connected to Internet. An Internet user can access, change, or delete susceptible information present on other computers with cruel intent or make for other users to some of the computer services engaged. The infrastructure of current computer networks is almost impossible to completely secure because such networks so vast and difficult. Therefore, an intrusion detection system (IDS) is needed to detect and reply effectively whenever the confidentiality, integrity, and availability of computer resources are under attack. Centralized Intrusion Detection (ID) models used by Most of the current distributed IDSs to make of individual host and network monitors along with a centralized controller component. The individual monitors send intrusion data to the centralized controller component and they perform analysis of the information it receives from each of the monitors. Following are some of the issues with the existing centralized ID models:

- Additions of new hosts source the load on the centralized controller to increase extensively. Because of it, it makes the IDS non-scalable.
- Platform specific components are presents in some of these IDSs.
- With the central component communication can overload parts of the network.

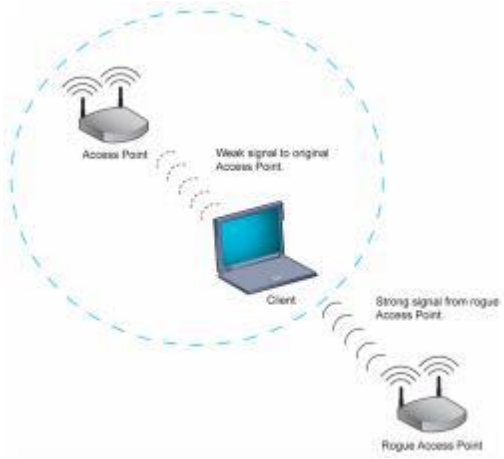

Figure 1 RAPs Higher Broadcast Power than Normal APs.

Having Rouge access points is risk threat for security of WLAN (wireless LAN). As per WLANs are more and more getting popular in last few years in network system? Threat to security of WLAN will lead to amount of loss for an association. Therefore comprehensive analysis of vulnerabilities of WLAN must be done and steps must be taken to strengthen security.

II. RELATED WORK

Although in investigating competent methods of detecting rogue access point in wireless LAN had lot amount of work has been done, this area still offers profusion of chance for further investigation in this regards as most of the answers available today are remote from satisfactory. The detailed information of related work has been mentioned below. Monitoring Radio Frequency waves and IP traffic are two big classes of methods to detecting rogue APs. Most presented saleable products take the first approach they either automate the process using sensors or physically scan the Radio Frequency waves using sniffers. Three recent research efforts also use Radio Frequency sensing to detect rogue access point, wireless clients are instrumented to collect information about nearby Access Points and send the information to a centralized server for rogue Access Point detection. The main idea of is to allow intense Radio Frequency monitoring during wireless devices connected to desktop machines. The trace on detecting protected layer- 3 rogue Access Points. The studies of detect rogue Access Points by monitoring IP traffic. The authors of established from experiments in a local test cot that wired and wireless connections can be separated by visually inspecting the timing in the packet traces of traffic generated by the clients. The technique in requires segmenting large packets into smaller ones.

➢ DRAWBACKS OF EXISTING WORKS

• Time consumption and detects rogue AP only when scanning is applied are drawbacks of Manual RF scanning. This plants sample range for an attacker to start attack and finish its work before he gets detected. This is severe ambiguity of this method.

• This approach also suffers from difficulty of scaling of network as it is not simply scalable.

• RF scanning method has considerable operation cost, and also scores less marks when it comes to effectiveness and correctness.

• High power consuming method is the Manual RF scanning. Consumption of power is an important parameter in mobile computing. Methods used in mobile computing should consume low power.

• Deployment cost is high and automatic scanning using sensors is less time consuming than manual scanning and provides a continuous attention to rogue Access Points. However, it may require a large number of sensors for good coverage.

III. SYSTEM ARCHITECTURE

The main purpose of the system is for the design an edge for detection of rouge access point in wireless LAN. We will be designing server model for organization Wireless LAN, which keeps track of every client, also fetch data from distant place, save it in database.

A. Mobile Agent Architecture

The method is planned for its system auditing implementation or independency on any operating system. Figure 2 shows the approach taken. A template-driven logic module analyzes the records for mistrustful activity. At the lowest level, the agent scans for events that are of attention independent of any past events. The agent scans each audit record created by the resident audit collection system. A filter is useful but it retains the records only those are of security attention. Those are altered into a homogeneous format which referred to as the host audit record (HAR).

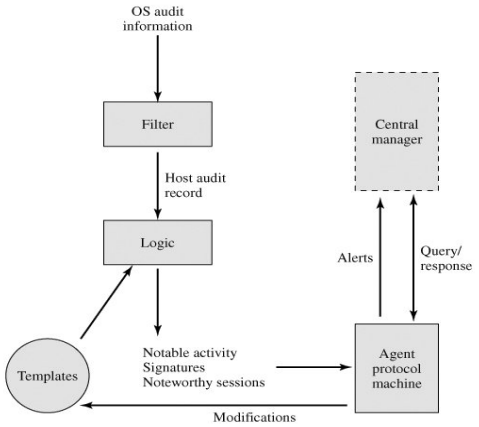

Fig 2. Mobile Agent Architecture

Mobile agents are computer programs, which may be independent, positive and reactive, and have the ability to learn. There is the progress from one node to another node and communicate with each other, allotment information to better carry out goals. Mobile agents broaden intelligence across the network, while pathetic in a network. The mobility

of mobile agents allows them to be created, deployed, and ended without disrupting the network arrangement. Mobile agents are computer programs, which are autonomous, proactive and reactive. Mobile agents extend intelligence across the network. The mobility of mobile agents, gives them to be created, deployed, and terminated without disrupting the network configuration. Mobile agent's programs creature sent across the network from the client to the server or vice versa. An agent that can be executing after being transfer over the network is being called. A software agent, called a software article that computerizes most of tricky tasks on behalf of human. The isolated programming using mobile agents is measured as a substitute to the conventional client-server programming based on the remote procedure e.g. CORBA. It is known by a life-cycle model. It is also known as a computational model. A software agent also called as a security model and a communication model. Although a mobile agent is also recognized by a basic agent model and navigation model. Following preliminary period of mobile agent, the present outlooks of research community from mobile agent are more challenging and practical. As after a decade of primary of mobile agents, it's clear that mobile are most excellent suitable for remote information reclamation. With the understanding & consideration of nature of mobile computing, usage of mobile agent happen to inescapable wherever computing hosts away from each other. And in such situation if we desire to know what is occurrence on remote host. Therefore the discovery of presence of RAP in wired, wireless or else hybrid type of network is a robust case for use of mobile agent for such detections. Therefore the mobile agent is fit for such case.

B. Architecture of Rogue access point detection using mobile agent

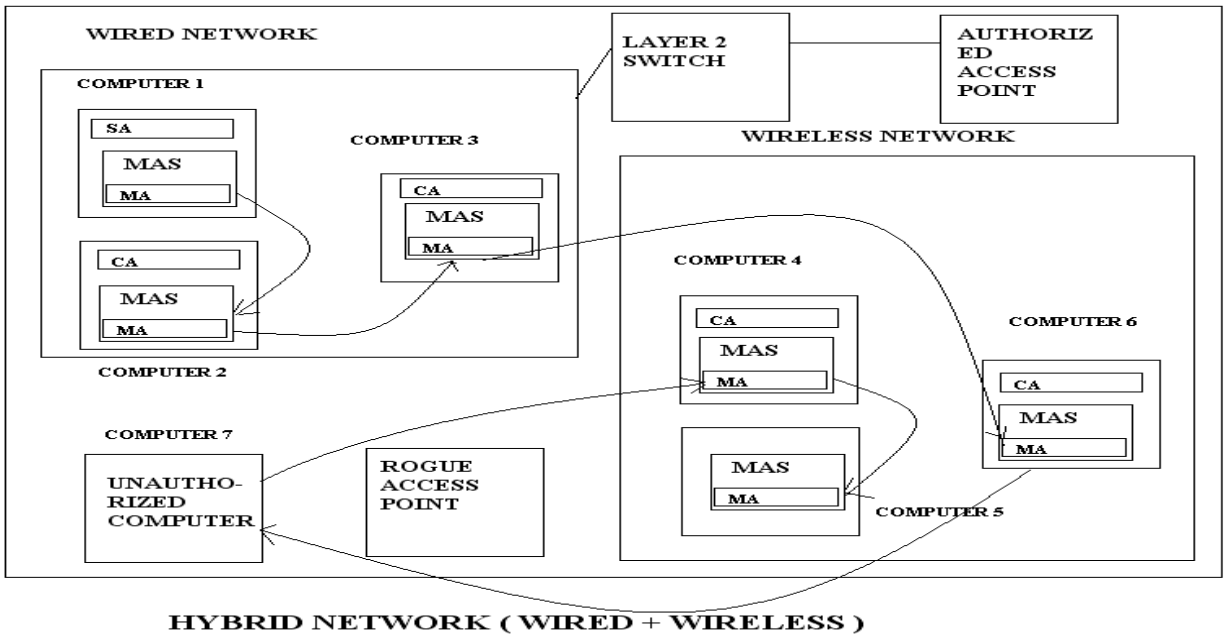

Fig.3 Mobile agent based architecture for rogue access point detection

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 inflate client-server software where server application (SA) will keep generate adequate long alpha numeric string after each minute, it will broadcast this string over whole network i.e. wired as well as wireless. At this time in this architecture we will systematize Server Application on server. Client Application will deploy on each authorized client in the network. Client Application will acknowledged to Server Application, each time it receive alpha-numeric key from Server Application. Client Application as soon as receive key from Server Application, stores in as text file on client on which it's deploy. Mobile Agent System deployed on all approved client in network. Whenever a new client will arrive in network, system administrator supposes to deploy Client Application and Mobile Agent System on these new clients. Merely following such operation these new clients will be permitted to operate in network. As shown in figure 1 in case-I attacker installs RAP either in NIC i.e. Network Interface Card, port or in switch port. Our goal is to detect this rogue access point. At the back this rogue access point

there will be unconstitutional client i.e. client 7. This client 7 will not have Mobile Agent System and Client Application installed on it.

IV. PROPOSE SYSTEM SCENARIO

At the beginning, alpha-numeric strings will be generated by SA following each minute and following will broadcast the key over whole network. Clients that are active at this time will trace these key strings and acknowledge them. At the same time Mobile Agent will begin from server. Server Application will save self generated alpha-numeric strings in file. Mobile Agent will take this from Server Application. MA will arbitrarily choose any lively client from network and will appoint that client. Say client 2 as shown in figure 1. After reaching as shown there, the mobile Agent will ask client 2 to give any past created alpha-numeric string. This assortment of past-generated key, might be ask, alpha-numeric key which is purely random in method so that attacker will face it difficult in guess the outline of alpha numeric string. As client 2 is an official computer, it will have alpha-numeric string with it and client 2 will generate it and will get legitimate. After this Mobile Agent will commencement for a different new client by using arbitrary client assortment method. Say client 3 as shown in figure 1. Just like client 2, as client 3 is also certified computer it will also get genuine by Mobile Agent. Following this Mobile Agent will again run arbitrary 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 severe crime and access point connected that client will be affirmed as rogue access point. In this method we managed to detect RAP. Following visiting every one computer Mobile Agent will return to server and will take recently updated file of alpha-numeric key from Server Application. After that it will once more keep visit clients in network in above mentioned behavior.

V. RESULTS AND DISCUSSION

A. USER INTERFACE

The basic user interface consists of at least two windows. First window is main window of system. It contains all the information about system and control of system. This window is divided into two frames. One frame is used to display the details of client, which are connected to the server like IP and MAC address of client. It also displays the status flag i.e. IDS flag and Block flag. The second frame displays the analysis part of the system. It has different graphs which are used to analyze the performance of the system. It also has facility to display the information of any client machine. Second window is GUI of Tahiti Server which displays the information of aglets. This window gives the user interface for creation, dispose, dispatch, cloning of aglet. The snapshots of all windows are as show in figures

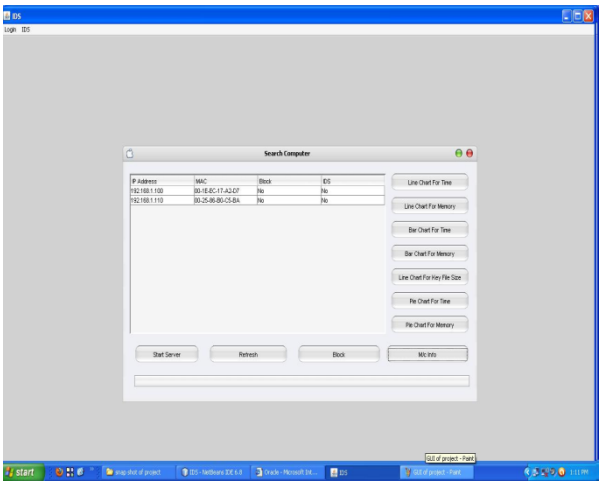

Fig 4. Main Window

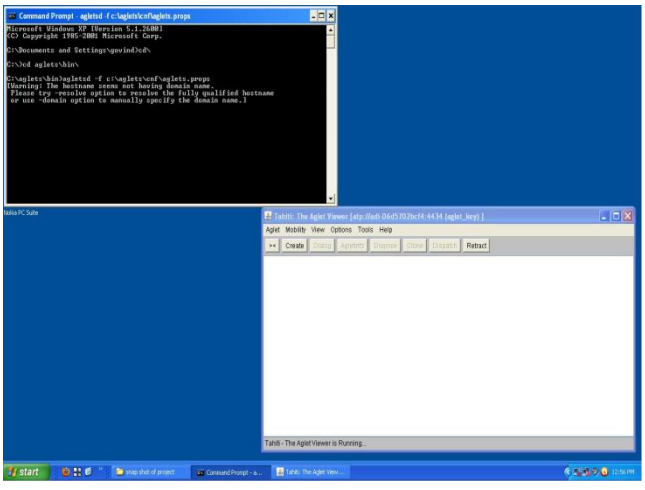

Fig 5 Tahiti Server

B. PERFORMANCE EVALUATION

In our test, we select two hosts established with WinXP /Vista operating system in a IEEE 802.11 WLAN to construct a distributed intrusion detection system platform based on Aglet. The hardware device is as follows: CPU: double P4, Memory: 1GB, Hardware: 80G. The host A acts as Manage Agent, other hosts B act as client. Their IP respectively is 192.168.1.100 and 192.168.1.104. Installed network should be considered as a trusted network. Server module will scan the network and get IP and MAC address of client through the aglet i.e. Mobile Agent. Server will generate the alphanumeric key after every one minute and that key will be broadcasted to the network by agent. Mobile agent will generate audit information at client side and send that information to the server. During this process the agent moves from server to client for analysis.

In the above performance evaluation, we examine the situation of CPU, memory utilization rate through system. The source utilization rate (CPU and memory) before and after this system running is shown in Figure 5.1. The experiment result shows the running of our system can't influence the host's normal work.

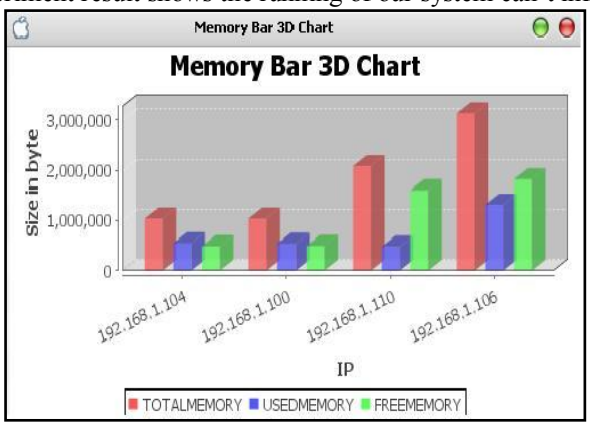

Fig 6 Comparison of Memory resources of Clients

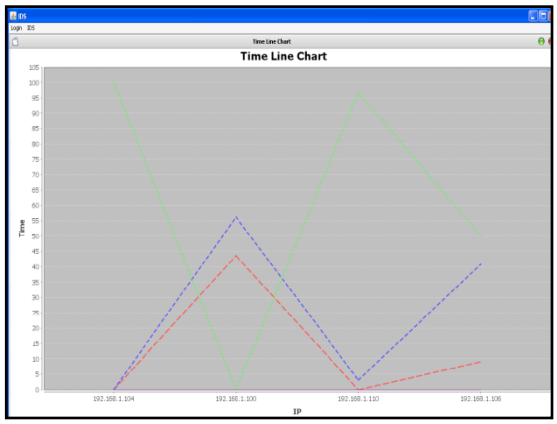

Fig 7 Comparison of System Time, User time and Idle Time of Clients

VI. CONCLUSION

In this System 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.

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.

