Using Multi-agent Sourcing Method for Detection and Elimination of Rogue Access Points in WLAN-802.11

Dnyanada S. Patil
Pune University
Smt. Kashibai Navale College Of Engg.Vadgaon(BK),Pune(India)

P.N.Mahalle
Pune University
Head, Computer Engg. Dept.
Smt. Kashibai Navale College Of Engg.Vadgaon (BK) ,Pune(India)

ABSTRACT

Due to the popularity of WLAN's there is tremendous rise in number of wireless attacks on Wireless LANs. Since, Security is a primary concern of any organizational network all threats to security of network must be eliminated properly before they cause harm to company network .One of such security threat is presence of rogue access point in the network. If these rogue access points are not handled properly in time may cause a serious loss to company network. Hence, there is need to detect and eliminate such rogue access points in the WLANs.

Proposed system provides a cost effective solution for detection and elimination of rogue access points in network. The system has such eminent properties that assure complete elimination of rogue access point & it does not require any specialized hardware or software for its use .Also does an automatic scan without human intervention saving user's time.

General Terms

Wireless LAN, Rogue Access point, Mobile agent, wireless network security

Keywords

Multi-agent, Clone Agent, Master Agent

1. INTRODUCTION

In order to extend the range of capabilities or services of an organizational network many organizations make use of WLANs. The WLAN allows communication between two nodes via an access point. These access points are specially configured nodes that act as a communication hub for wireless LAN user. An Access point provide mobility to current capabilities of network services such that users can roam around within local coverage and still have access to the network services. With the advantages of mobility, flexibility, portability the issues of network security and performance must also be considered .Employees within the organization may also deploy their own access points for company use without explicit authorization (called Rogue Access Point). But later there are chances where employees may misuse these access points for their own benefit. This easily causes the chances of confidential information to be revealed to third party. Such security threats create internal threat to organizational data and network.

Dealing with these rogue access points is very challenging because people with less security background can also misuse these access points for their own benefit. Where as in case of other security attacks the attacker requires either very high level of knowledge or may require use of expensive devices. Even if these rogue access points are installed by valid users still it results into the security hole for a network. There are many different categories of rogue access points such as unauthorized, improperly configured, phishing, compromised and related possible scenarios. It is essential to detect and eliminate these rogue access points in time and maintain the security of network [1] [2].

2. Motivation:

Rogue access points are installed within an organizational network without explicit permission from local network administrator, which in turn might cause an intruder to conduct Man-in-the-middle attack. Such access points may cause a severe loss to organization. Because anyone with access to local coverage can ignorantly install their own access points or devices within company network and allow access to network information to third parties.

If proper and compelling authentication security policies are employed within network then there are very less chances of unauthorized users getting access to sensitive corporate data. But risk of such threat increases when employees within organization deploy their own access points in network.Employees have free access to all network services due to that they may install their own access points unknowingly and can utilize services of network for their benefit. This causes a greater risk for an organization from security point of view.

To avoid such situation it is necessary to implement security policies that assure network security and mandates coordination with network administrator to deploy access points in network [7].It is easy for intruder with less technical background to easily access corporate network and hence to avoid the risk of network security it is necessary to develop a system that detects and completely eliminates rogue access points in network.

3. Related Work:

As discussed above 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 network access points 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. [2] Gives classification of various access points and also describes the design using distributed monitoring module framework. Authors of [3] 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.[4] Describes approach to secure data using frame collectors

and mobile agents to detect rogue access devices in wired and wireless environment. Authors of [5] proposed an approach to detect rogue access points in distributed environment using mobile agents. [6] describes an 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 [7] 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.[8] 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.

Plenty of work is done in detection and elimination of rogue access points. There are various solutions to detect and eliminate rogue access points.

3.1 Currently used tools and their drawbacks:

3.1.1 NETSTUMBLER:

NetStumbler is a tool that makes it easier to detect 802.11 a/b/g WLAN standards. While war driving is its main use, this application also facilitates verifying network configurations. It makes you find locations that suffer from weak signal within a WLAN, detect issues of wireless interference and rogue access points. Thus, user is able to target directional antennas in order to benefit from extended wireless signal quality and strength.

Disadvantages:

1. It does not work with every known Wi-Fi adapter.

2. It does not analyse non Wi-Fi signals. If you have a cordless phone, microwave oven, or nearby radio operator,

NetStumbler will show those merely as "noise", as part of the signal to noise ratio for any Wi-Fi network device.

3. NetStumbler binds to the Wi-Fi adapter just like any other Wi-Fi client. If you run NetStumbler while you're attached normally to your network, using Wi-Fi, you'll experience the same instabilities as when you run multiple Wi-Fi client managers.

4. Netstumbler is not compatible with Windows Vista

5. No updated version has been developed since 2005.

3.1.2 AirSnare

AirSnare is a program for Windows that helps you detect DHCP requests or unauthorized MAC addresses trying to connect to an AP. In case of unauthorisedd MAC address or DHCP request the intrusion response consists of an alert to the administrator and optional message is sent to the intruder via Windows netmessage. AirSnare has a non-commercial license.

Disadvantage:

Due to excessive load of network accesses there are chances of main server failure. In such cases server hangs and tool stops working and this is not useful in case of frequent DHCP server requests.

3.2 Use of mobile agents:

Mobile agents can also be defined as programs that perform certain tasks on behalf of the user [12]. While dispatch of clones at several nodes require migration from one place to another which is not possible efficiently with other systems. In a network when an agent migrates from one level to other it also consists of the program code and the program execution state. It is now clear that mobile agents are best suited for remote information retrieval so even if the access point is far away still it is possible to monitor its status by use of mobile agents. To determine authentication of a node in network mobile agent executes a specialized code at each node in the network. Along with this the mobile agents have following properties which make the system fast and fault tolerant:

1. Intelligence
2. Autonomy
3. Responsiveness
4. Adaptability

3.3 Detection and elimination of rogue access point WLAN:

The system is a multi-agent based methodology which not only detects rogue access points but also eliminates 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 for organizational network security threats. This proposed technique can detect and eliminate access points both in form of rogue access point as well as in the form of rogue clients acting as a rogue AP.

With the survey of existing system it is been observed that the available systems require manual scan of entire system which requires lots of time. Scanning each node manually is a tedious task. It basically have a layered architecture to support multi-agent architecture that contains mobile agents at two different levels one as master agent and another as client/slave agent. The master is created automatically which in turn produces the slave agents at each access point in the network. The job of slave agent is to produce slave clones depending on number of access points in the network and dispatch them to clients connected in the network. These clones in turn will execute the code for access point authentication. If clone fails to find match of information then the access point is blocked and it is also added to the list of invalid access points at central master repository.

4. DESIGN

4.1 DHCP enabled network:

In the proposed system the most crucial element is DHCP enabled network. Since two different levels of mobile agents are assumed: master and slave. The DHCP enabled systems is used for allocating IP addresses. At very initial stage only master agents are produced which in turn produce slave agents for their respective clients depending on the number of access points in the network. The master is capable of regulating all authorization in wireless network. Initially it will have list of all valid and registered access points in the network. The master and slave agents

both work in coordination for detection and elimination of rogue access points in the network. It considers the number of active access points in the network and accordingly generates slave agents. The entire system will be dependent on this central server. Since this central system will maintain all the details of valid access points & in order to authenticate those points they must be registered with DHCP-server.

4.1.1 Functions of DHCP enabled network:

- ✓ Registering & deregistering access points, client cards & agents
- ✓ Scanning the network
- ✓ Acting as a server for whole wireless network.

When an agent is registered it will add the agents info, name, IP, location, MAC address to its database. In turn administrator sends this information to all other agents for communication purpose. When it deregisters agents it simply removes agents record from its list of agents.

4.2 Agents:

Agents are main building blocks of system. These agents keep migrating at client side and help you detect RAP's. Agents perform prominent job of detecting unauthorized wireless elements like rogue access points in network. Also they act as a first line of defense to protect the network from unauthorized use of network resources.

4.2.1 Functions of agents

- ✓ Accept registration & deregistration messages for AP's & client cards from the CA
- ✓ Keep scanning the cells for RAP & notify the concerned personnel if found.
- ✓ Block unauthorized AP's
- ✓ Maintain list of registered AP's in the network.

4.3 Client:

Clients shown in the figure 1 are nothing but the wireless nodes that access the network data and services through access points present in the network. These clients are dynamic in nature since they are wireless nodes they continuously change their position in network and have access to network services & data via different access points.

5. OVERVIEW OF ARCHITECTURE:

5.1 Registration and deregistration:

To identify the valid access points, clients and agents in network they must be registered with the central administrator. To register them basic information is required that is a prominent part that determines the identity of access point in the network. To register them an encryption algorithm is to be used which will compute the keys for:

1. Individual Node
2. Access point
3. Unique key between wireless client & access node

By computing these keys when an clone agent will try to execute the authentication code at access point node if it executes that code successfully for getting MAC address of the machine and its SSID etc. then the access point is found to be valid one, otherwise it is an invalid access point.

5.1.1 Detection algorithm:

An access point is first registered in the network. When a new access point is found in network a clone of slave is dispatched to associated client node. Detection algorithm is applied to determine whether the access point demanding the network services is valid or not. To determine this master agent generates its slaves which in turn will generate and dispatch its clones to respective access points present in the network. If the MAC address of the access point and SSID of access point in

6.1 Implementation:

With the prior permission and rights from the network administrator clients may deploy their own access points in network. But the purpose of proposed system is to detect such access points that are deployed without explicit authorization within network. Initially an DHCP enabled network will assign addresses to the network nodes which will act as a master agents of system. Based on number of access points master agents will create slaves in the network. The clones of those slaves are created and dispatched to individual access

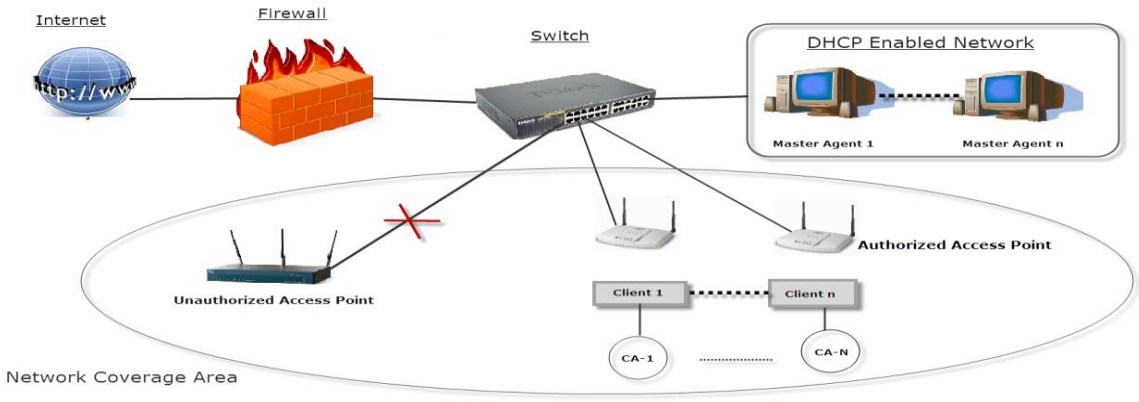

Fig 1: System Architecture CA-1 means clone agent for client 1 and so on.

info packet matches with the information registered in central repository then the access point is randomly connected to the network via an AP through which those clients can access network services. But also there is one access point which also provides same network services with more strong signals to the clients which is nothing but a fake way by which that access point will have access to confidential data of clients and this may cause serious harm to organizational data.

6. Proposed Architecture:

Under the proposed architecture multiple master agents are generated depending on the size of network. If numbers of nodes in the network are more than 10 then the system will automatically generate third master agent to overcome the problem of network load on single master. The DHCP-server will maintain the central repository then the access point is said to be valid. But, if the information does not match then the port from where the MAC address is obtained is blocked. points in network. When clone slave agent finds presence of any new access point it automatically sends information packet containing (SSID,MAC address, vendor name, medium used, etc.) to clone agent of access point. Active slave agent at AP in turn informs or sends the same to master agent. Master agent verifies the information provided from central repository. Master agent verifies whether address sent is of access point or client in network. If address is found to be of access point it is considered as authorized or valid access point. If address sent is of client an isolation frame is sent to all access points to inform all not to connect with that client. Otherwise the access point is considered as unauthorized access point and the port from which MAC address is connected is seeked and it is blocked.

7. Results & Discussion:

Results would be based on following parameters:

1. Perfomance Measurement:

Measurement of performance parameters such as end-to-end delay, network load ratio, throughput when system operates at normal mode.

Measurement of performance parameters such as end-to-end delay, network load ratio, throughput when system detects a rogue access point and goes under its avoidance procedure.

Performance comparison between normal mode network and presence of rough access point detection and avoidance process

2. Generation of multiple master agents:

Since proposed architecture overcomes the drawbacks of single master agent system here focus is on finding out the traffic & network load on individual master system if there are more than 10 access points which fully overloads the master agent then system would automatically find master agent which is idle or has less network load.

8. Conclusion & future work:

With the rapid use wireless LANS it is required to secure organizational network. The proposed approach overcomes the disadvantages of current approaches and provides cost effective solution to the problem. Along with the detection the rogue access points are eliminated without specialized hardware. Most of the internal threats to organizational security will be removed and it will increase the flexibility of accessing network services within network area. The manual work of administrator to search for rogue access points and eliminating them will be reduced to a large extent.

Future work includes the development of system and its further survey to find effectiveness of system from user's point of view. The results will be compared based on

9. REFERENCES

[1] V. S. Shankar Sriram, G. Sahoo, Ashish P. Singh, Abhishek Kumar Maurya "Securing IEEE 802.11 Wireless LANs - A Mobile Agent Based Architecture" 2009 IEEE International Advance Computing Conference

[2] 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* distributed system" CSCIT,Nanded on 09 Jan 2010.

[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] 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 Journal of Advanced Engineering Technology E-ISSN0976-3945 IJAET/Vol.III/ Issue II/April-June, 2012/127-130 Research Article

[5] Prof. Suryawanshi Govind R,Prof. S.B.Vanjale "Architecture of mobile agent for Distributed rogue access point detection in distributed system" CSCIT,Nanded on 09 Jan 2010.

[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 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.

[8] 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

[9] MS.SnehalBehede,S.B.Vanjale,P.B.Mane"Provoding data security in WLAN by detecting unauthorized access points and attacks"Intenational Journal Of Engineering Science And Technology.

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

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

[12] http://www.softpedia.com/get/NetworkTools/Network-Monitoring/NetStumbler.shtml
[13]www.ias.ac.in/resonance/July2002/pdf/July2002p3543.pdf

[14]http://www.engeniustech.com.au/EnGeniusV2/knowlage.php?itemAppId=28