IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

Fake Access point and Invalid Client Detection Elimination Using Agent Multi sourcing

Miss. Prachi M. Kharat[1], Prof. N. D. Kale[2]

PG Student, Comp. Engg, PVPIT, Pune, India [1]

Assistant Professor, Comp. Engg, PVPIT, Pune, India [2]

Abstract: 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. Rogue Access Points (RAPs) is one of the primary security threads in current framework circumstance, if not honestly dealt with in time could lead from minor framework issues to genuine system network failure. We propose a Multi-Agent Sourcing Based Methodology, which recognizes Rogue Access Point as well as totally eliminates it. This Methodology has the going with phenomenal properties: (1) it doesn't require any particular equipment or hardware; (2) the proposed calculation identifies and totally disposes of the RAPs from system; (3) it provides a cost-effective solution. The proposed procedure can block RAPs and also remove them from the systems.

Keywords: WLAN, RAP, Multi-Agent Source.

I. 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. [2]There are number of wireless attacks which may severely harm organizational network and security of 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 users 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.[1] [4] [11] [12]The entrance point is a point which is a computer's software product that goes about as a communication center for clients of a remote device to associate with a wired LAN.

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.[9] 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 [1] [5] 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.

II. 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 determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external 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.

A. 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.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

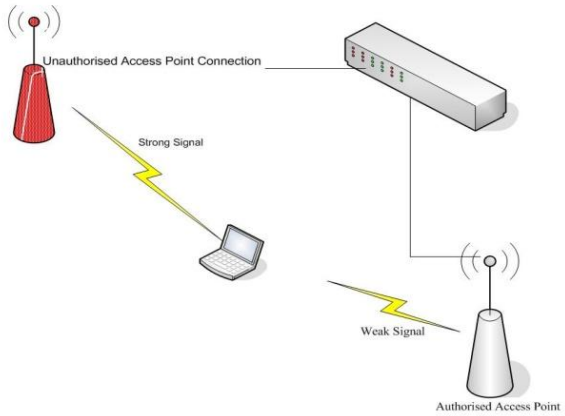


Fig1: Wireless network scenario

B. 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.

TCP Fingerprinting

In this method, various specially crafted packets are used to examine the behaviour 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.

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.

Packet Sniffing

In this method a device is configured to run in promiscuous mode and analyse 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:

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 respond 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.

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

C. 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.

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.

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.

AirMagnet

AirMagnet 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

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. [19]

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].

III. 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.

IV. 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.

A. 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.

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.

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.

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

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

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.

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.

V. DATA FLOW DIAGRAM

In this section we are going to discuss the DFD i.e. (Data Flow Diagram). This diagram shows the complete overview of the each module in the project. Also shows how exactly data flows in the total system.

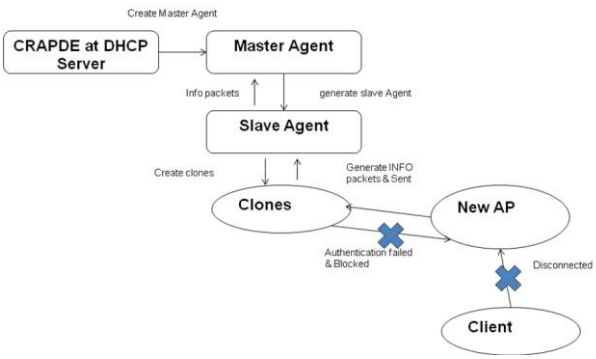


Fig2: Data Flow Diagram

VI. SYSTEM ARCHITECTURE

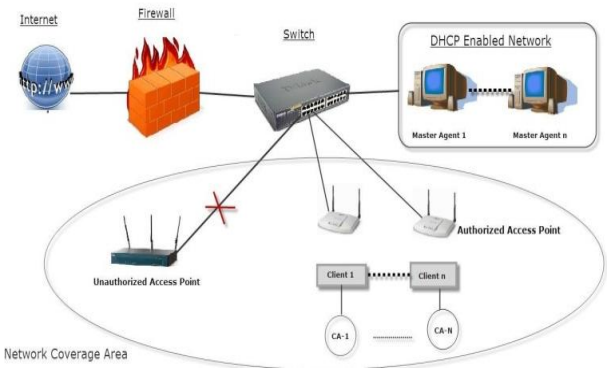


Fig3: System Architecture

Fig.3, gives abstract view of proposed system. This system architecture represents different system components involved. 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.

A. Advantages of System

▪ **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.

▪ **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.

▪ **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.

▪ **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.

B. Algorithmic Steps

a. 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.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

VII. MATHEMATICAL MODEL

A set is defined as a collection of same type of class of objects.
Let S be the system:
where

Mobile agent
Set (M) = {O; 1; 2; 3; 4; 5}
0 = Spawn N thread as the number of clients in the cell
1 = Fetch Audit information from the client Machine and send audit information to Server.
2 = Compare alphanumeric keys at server and client side
3 = If comparison is true set flag=1.
4 = Notify central administrator for IDS Detection alert.
5 = Request Blocking that Client. Otherwise, set flag=0

Sever Application
Set(S) = {7; 8; 9; 10; 11; 12}
7 = Upload mobile agent
8 = Wait for notification of possible alert from agents of cells
9 = Search for corresponding IP Address from database.
10 = Inform that the system is attacked to administrator.
11 = Perform scanning of network and add information of client after every one minute to the database
12 = Broadcast same key to network using MA

Mobile Agent System
Set (P) = {13; 14}
13 = Upload mobile agent system on client
14 = Show alphanumeric string to Mobile agent
1) MUS = {0, 1, 2, 3, 4; 5, 7, 8, 9, 10, 11, 12}
2) MUP = {0, 1, 2, 3, 4, 5, 13, 14}
3) S UP = {7, 8, 9, 10, 11, 12, 13, 14}
4) M∩S = {3, 5}

VIII. RESULT

A. 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.

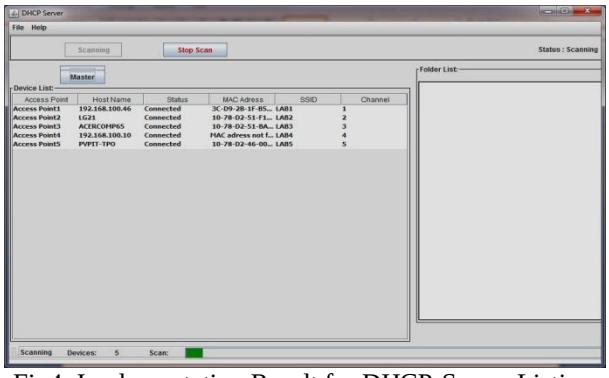


Fig4: Implementation Result for DHCP-Server Listing

Access Points

Fig, 4 shows implementation result for scanning wireless network that displays the list of all access points connected to network. The DHCP server generates a master agent that gives detailed list of all connected access points along with their IP address, MAC address, SSID etc. The process of network scanning lists all necessary details of each access point in wireless network including Host Name, Status, MAC address, SSID and channel used by access point. Host name is nothing but the IP address or name given to each access point. Status gives details of access point signifying whether it is connected/disconnected to network or it is blocked from network.MAC address specifies the physical address of each access point which is another crucial parameter which determines validity of access point in network. SSID is unique Service Set Identifier for each network and generally it is same for all wireless nodes in entire network. Normally it is a human-readable text string and commonly known as "network name". All wireless devices must have same SSID in order to communicate with each other. Channel is the medium through which wireless device is connected to network or it is a physical transmission medium.

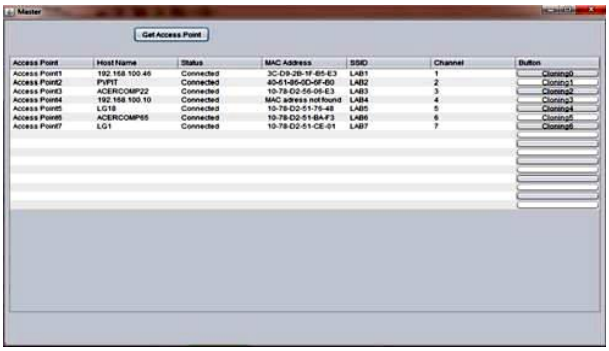


Fig5: Master Agent Gets the List of Registered Access Points

Fig.5 shows implementation of master agent listing registered access points that are connected to network. When master agent is generated by DHCP server it gets the list of all registered access points in network. The scanning process, authorization process of access points is conducted by master agent. Generation of slaves and their clones at each access point, determining validity of access points and accordingly taking security related decisions are some of the main functions of master agent.CMS scheme produce multiple master agents to prevent system from master agent failure because if central master agent fails entire system will fail. In order to prevent system from total failure an alternate master agent is generated so that in case of failure newly generated master agent would take control of system and start monitoring it. This reduces the chances of system failure and makes it fault tolerant. During network scanning process master agent continuously communicates with its slaves and their clones to get the information about malicious AP's. If such fake access points are detected they are immediately blocked or eliminated from network. CMS scheme makes system

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

very flexible and easier to operate. Above figure illustrates the process of getting list of registered access points in network and allows master to generate slaves and clones for those access points.

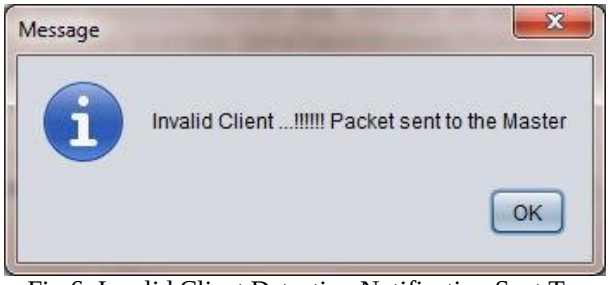


Fig.6: Invalid Client Detection Notification Sent To Master

Fig. 6 shows the case where invalid client packet is found and it is sent to the master. This informs master agent about the presence of invalid or unauthorized access point in network. When master agent receives this message from clone agent it immediately executes elimination or blocking algorithm where MAC address of access point is fetched and port from where MAC address is connected is searched. Once the port is found it is blocked so that access point is no longer a part of wireless network and the same is informed to all its clients to reduce chances of third party attacks in network clients.

B. Certainty Analysis

The certainty analysis is the notion of risk discount to be subtracted from the expected yield.

1. Proper load balancing or scheduling methodology can be implemented.
2. The MAC address and SSID of already blocked access points can be maintained and checked every time they appear.
3. By using encryption algorithms packet integrity can be checked when it was sent and accordingly it can be judged.

The above certainty analysis can be more described by graphs shown below:

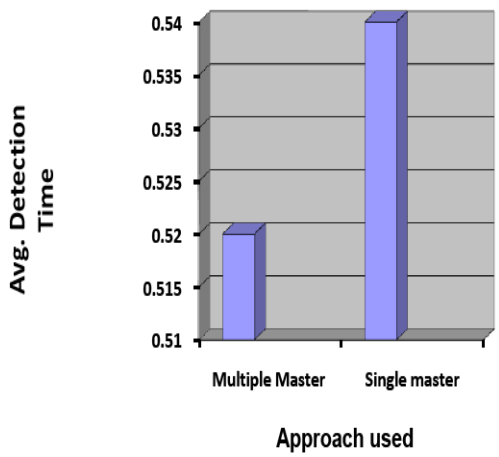


Fig7: Average Detection Time

Above graph shows the performance of detection time required by existing system which uses clock skews for detection of rogue access points in network. The ranges of values are for throughput to measure the overall performance of system. With multiple master agent approach the system gives better performance.

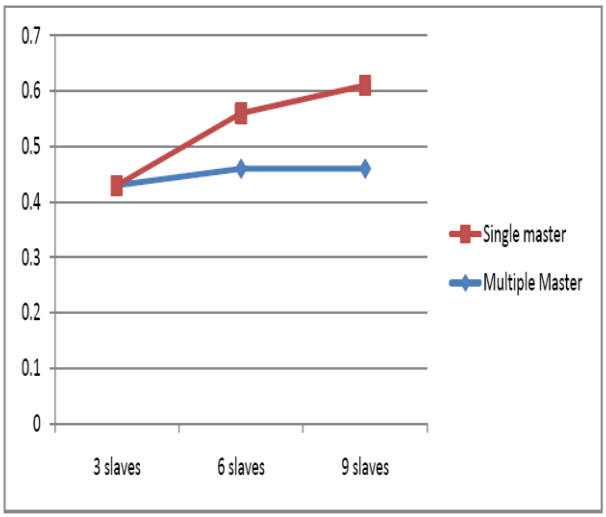


Fig8: End to End Delay (Seconds) Performance

Above graph shows the end-to-end delay performance for single master agent and the performance of CMS scheme. For single master agent approach as number of slaves increase the performance degrades whereas for multiple master agents as number of slaves increases performance is not affected. The time taken by packet to move from source to destination is the end-to-end delay of network packet .The proposed approach gives reduced end-to-end delay so that overall time required for transmission of INFO packet is also reduced this results into quick detection of fake access point for a network.

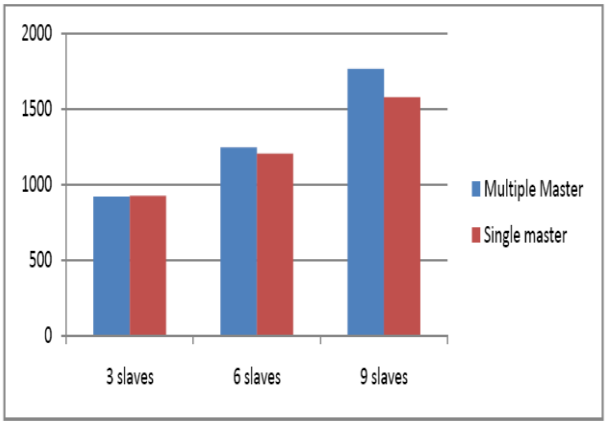


Fig.10: Throughput (KBPS) Performance

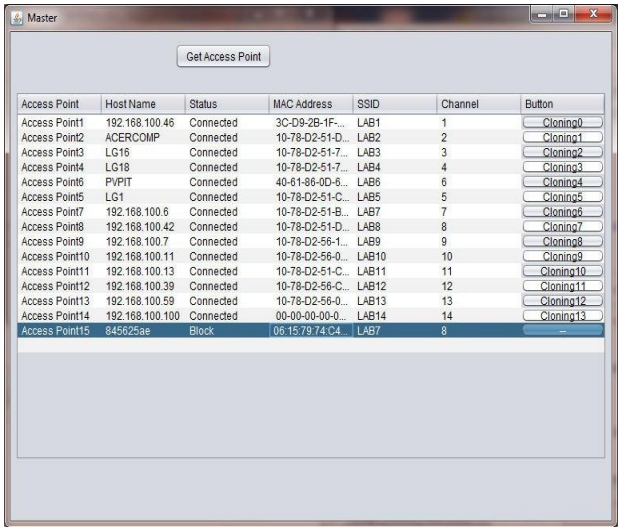
Above graph shows the overall throughput of system where the performance of both systems can be easily compared. As there is increase in number of slaves the CMS scheme works better than existing single master agent system. Here throughput measurement is done to check efficiency of proposed system with multiple

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

masters. From above graph we see that if numbers of slaves are more than performance of multiple master agent schemes is little high than single master agent system but as number of slaves increase performance of single master agent system degrades and at the same time performance of multiple master agent schemes is increased.



Access Point	Host Name	Status	MAC Address	SSID	Channel	Button
Access Point1	192.168.100.46	Connected	3C-D9-2B-1F-...	LAB1	1	Cloning0
Access Point2	ACERCOMP	Connected	10-78-D2-51-D...	LAB2	2	Cloning1
Access Point3	LG16	Connected	10-78-D2-51-7...	LAB3	3	Cloning2
Access Point4	LG18	Connected	10-78-D2-51-7...	LAB4	4	Cloning3
Access Point6	PVPIT	Connected	40-61-86-0D-6...	LAB6	6	Cloning4
Access Point5	LG1	Connected	10-78-D2-51-C...	LAB5	5	Cloning5
Access Point7	192.168.100.6	Connected	10-78-D2-51-B...	LAB7	7	Cloning6
Access Point8	192.168.100.42	Connected	10-78-D2-51-D...	LAB8	8	Cloning7
Access Point9	192.168.100.7	Connected	10-78-D2-56-1...	LAB9	9	Cloning8
Access Point10	192.168.100.11	Connected	10-78-D2-56-0...	LAB10	10	Cloning9
Access Point11	192.168.100.13	Connected	10-78-D2-51-C...	LAB11	11	Cloning10
Access Point12	192.168.100.39	Connected	10-78-D2-56-C...	LAB12	12	Cloning11
Access Point13	192.168.100.59	Connected	10-78-D2-56-0...	LAB13	13	Cloning12
Access Point14	192.168.100.100	Connected	00-00-00-00-0...	LAB14	14	Cloning13
Access Point15	845625ae	Block	06:15:79:74:C4...	LAB7	8	--

Fig.11: Detection and Blocking of Invalid Point

Fig. 11 shows detection and blocking of fake client in wireless network. The above figure highlights the blocking of invalid access point in network. Once the blocking algorithm is executed the access point along with its host name, Status, MAC address, SSID and channel no. is displayed. When access point is blocked its status is set to "BLOCK" which gives confirmation that the invalid or fake access point in network is blocked.

IX. EXPERIMENTAL SETUP

A. Defining Requirements for New System

The 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.

B. 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.

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.

C. Result

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.

Outcomes Invalid Access points are identified and blocked.

X. 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.

ACKNOWLEDGMENT

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 up to its completion. My sincere thanks to the Head of the Department of Computer Engineering **Dr. B. K. Sarkar** sir who continuously motivated and guided me for completion of this paper. I am also thankful to all teaching and non-teaching 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.

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] 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.
[4] 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
[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 Journal of 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 on 09 Jan 2010.
[7] Suman Jana and Sneha K. Kasera "On Fast Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews IEEE Transactions on mobile computing, Vol. 9, No.3, March 2010
[8] LanierWatkins, Raheem Beyah, Cherita Corbett "A Passive Approach to Rogue Access Point Detection 2007 IEEE
[9] 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
[10] Sandeep, Rachna Rajpoot,"Detection of Fake access point in wireless LAN network:A review, (IJSETR), Volume 4, Issue 5, May 2015
[11] Mehndi Samra, Mehak Mengi, Sparsh Sharma and Naveen Kumar Gondhi, "Detection and mitigation of rogue access point, Journal of Scientific and Technical Advancements, Volume 1, Issue 3, pp. 195-198, 2015.
[12] Ms. Swati Jadhav, Prof. S.B.Vanjale, Prof.Dr. P.B.Mane, "Illegal Access Point Detection Using Clock Skews Method in Wireless LAN,IEEE 2014
[13] NetStumbler- http://www.netstumbler.com
[14] AirMagnet-http://www.airmagnet.com
[15] http://www.softpedia.com/get/Network-Tools/Network-Monitoring/NetStumbler.shtml
[16] http://www.leger.ca/pages/CHAMPLAIN/WLAN-tools.htm
[17] www.ias.ac.in/resonance/July2002/pdf/July2002p35-43.pdf
[18]http://www.engeniustech.com.au/EnGeniusV2/knowlage.php?itemAppId=
[18] http://www.kismetwireless.net