



To Detect Unauthorized Access Point in WLAN Using Advanced Internet Proxy

Amol S. Papade¹, Vikas E. Pansare², Rohit D. Patil³, Prof. S S.Gore⁴

B.E. Students, Dept. of Computer, Jaihind College of Engineering, University of Pune, India^{1,2,3}

Assistant Professor, Dept. of Computer, Jaihind College of Engineering, University of Pune, India⁴

ABSTRACT: Illegal Access Point which is called as Rogue Access Point (RAP) is an access point that has been installed on a secure network without explicit authorization from a system administrator. Wireless Networks has big security threat called Rogue access points. If care is not taken and if this network threats are not detected and mitigated on time, this will result into the serious network damage and data loss.

Rogue access points, if undetected, can be an open door to sensitive information on the network. Many data raiders have taken advantage of the undetected rogue access points in enterprises to not only get free Internet access, but also to view confidential information. Most of the current solutions to detect rouge access points are not automated and are dependent on a specific wireless technology. The approach is an automated solution which can be installed on any router at the edge of a network.

The main objective of this project is to develop software with functionality of Rouge Access Point Detection & Counter Attack using Advanced Internet Proxy. The contribution of this project is a novel approach to detect Rogue Access Points in a Network using Elimination of Intrusion Detection.

KEYWORDS: WLAN, Rogue AP Security .

I. INTRODUCTION

Rogue Access Point detection is a two step process starting with discovering the presence of an Access Point in the network and then proceeding to identify whether it is a rogue or not. The presence of Rogue Access Point (RAP) is major security concern in wireless network. If this kind of security threat is alive into WLAN, it results into leakage of confidential information to outside network. In our implementation, we have make used of clock skew of wireless LAN access point as its fingerprint to detect the fake APs. Fingerprinting will act as unique identification like human fingerprint work. The major objective of using the clock skew interval for detecting the fake AP is to overcome the limitation of existing approach. Existing methods for detection of fake AP has limitation of detecting MAC address spoofing.

- A rogue access point (AP), also called rogue AP, is any Wi-Fi access point that is installed on a network but is not authorized for operation on that network, and is not under the management of the network administrator.
- In this project proxy server is playing an important role. This proxy server will run on server machine. The client will run the project. There is one more class that run and fetch the all machine details. These details are then store at database. While checking whether the request is authorized or unauthorized, proxy cross check with database and as per details it will give the access to internet.
- At that time check for the IP spoofing too. In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. That means in this project, we are checking whether two machines has same IP, if yes then one of them must be fake. For this we are storing all machine details in database.
- An authorized user can have internet access and unauthorized is unable to access the internet. The admin will handle the things, such as allow or deny the particular user, block the port number, view the login details etc.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

- Rouge Access Point Detection & Counter Attack is desktop application. In which, we are going to detect access point first and check whether this AP are rouge access points.
- Here we are also detecting the IP Spoofing. For this the machine details like IP address, Media Access Control(MAC) address , Hard Disk Serial number etc. are stored at database and when request come it should go through proxy and then proxy will check that request is authorized or not. If it is rouge then the port number of that particular client will be blocked. So that it won't have access in future.

II. PROPOSED SYSTEM

This is the proposed system which is simplified networked model with access point and sniffers.

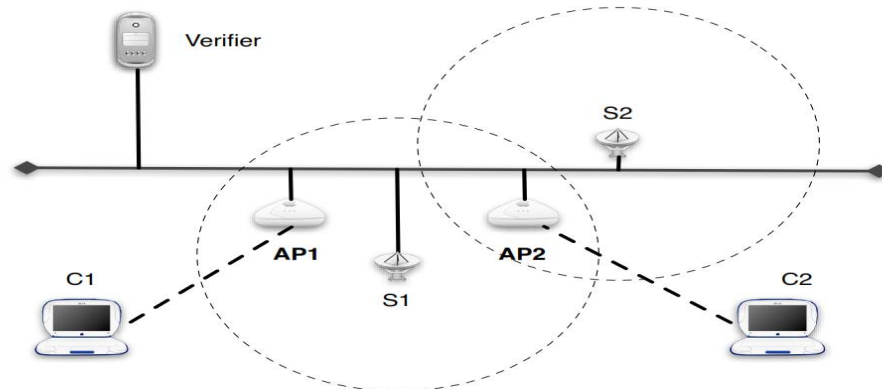


FIG 1. A SIMPLIFIED NETWORK MODEL WITH AP'S & SNIFFERS

The system architecture is depicted in Figure 1 and was implemented as a client-server architecture using off-the-shelf commercial hardware and an open-source Wi-Fi sniffer. A modified version of was built and installed in a number of monitors as clients. These clients measure AP data transmission and signal characteristics. They then report their measurements to the server which detects and locates rouge APs if present.

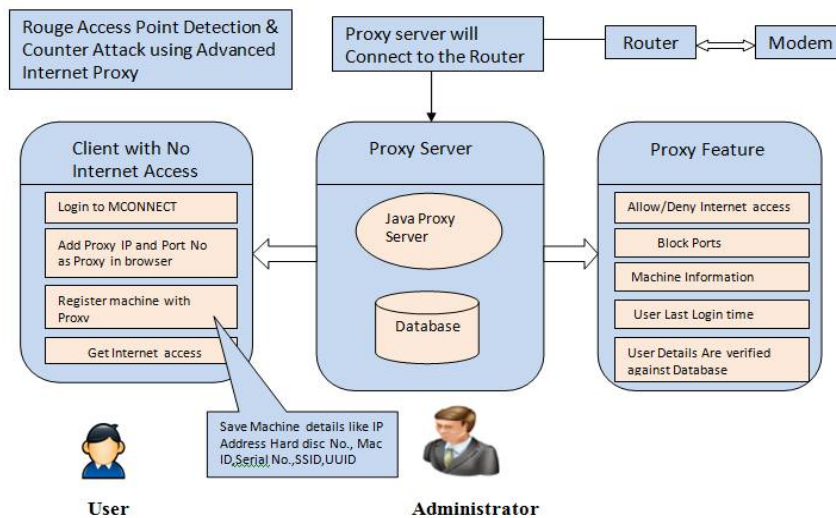


Fig 2. System Architecture



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Client monitors, whose locations are set in the table below the map. The identified rogue APs are shown on the right hand side table, and represented by the orange dots on the map.

III. PRODUCT FEATURES

- **Proxy**

1. All hosts have to go through proxy server.
2. Proxy will detect hosts MAC_ID, SSID, IP Address, Hard disc serial no and requested port no as per incoming requests.
3. Host policies and rules are stored in the MYSQL database on proxy server.
4. Proxy will check the host policy and process the request accordingly.
5. Proxy Features are:
 - a. Allow/Deny Internet Access.
 - b. Block Incoming/Outgoing Ports.
 - c. Catch Machine Information.
 - d. Maintain user login information.
 - e. Detect Rouge Access Point.

- **Server**

1. Admin can view login details.
2. Admin can define rules for the host and allow/deny them for internet access.
3. Admin can add ports to incoming/outgoing port list.

- **Client**

1. Client has to Start Application.
2. Login with your credentials.
3. Set the proxy IP and port no in browser proxy Hit web URL to connect to.

IV. RESULT SECTION

Here we provide input to the proxy server that is the proxy IP.



Fig 1. Input To Proxy Server



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

After successfully accepting the valid proxy IP then user gets proxy server details will be displayed on screen.



Fig 2. Proxy Server

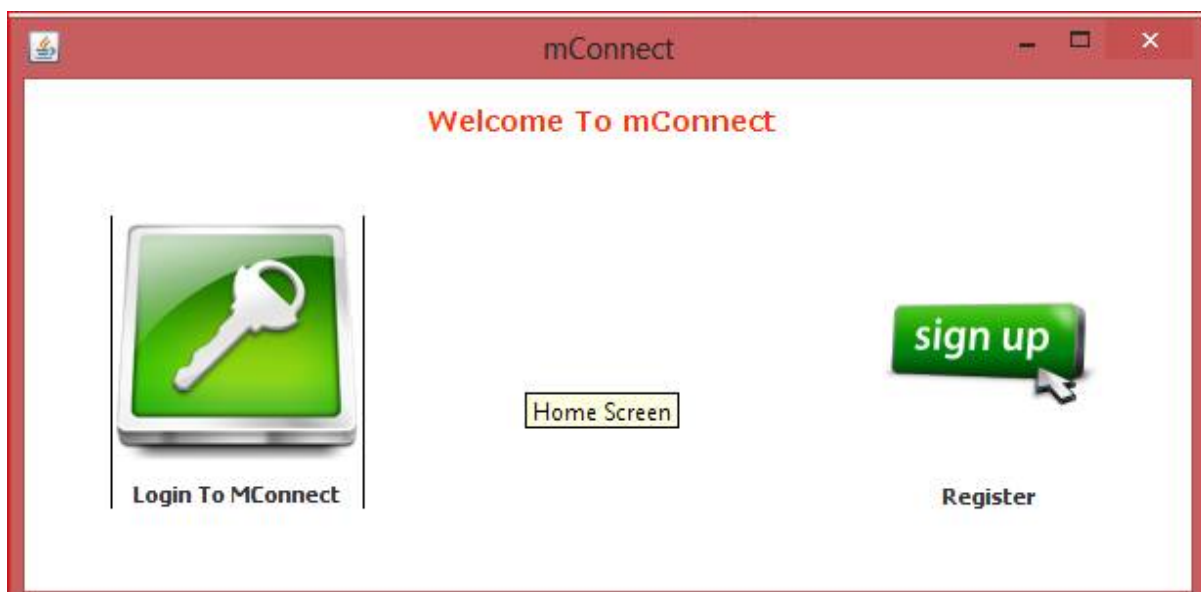


Fig 3. Home Screen



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

mConnect

mConnect - Register Screen

User ID

Name

Password

Re - Enter Password

 Register  Reset Form

Fig 4. Registration Screen

mConnect

mConnect - Login Screen

User Name

Password


 Secured Login  Reset

Fig 5. Login Screen

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

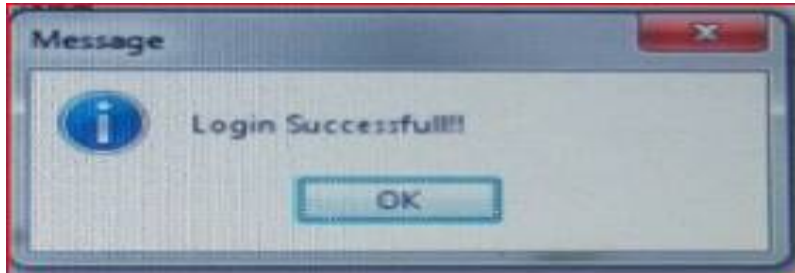


Fig 6.Login Successful



Fig 7.Client Home Screen

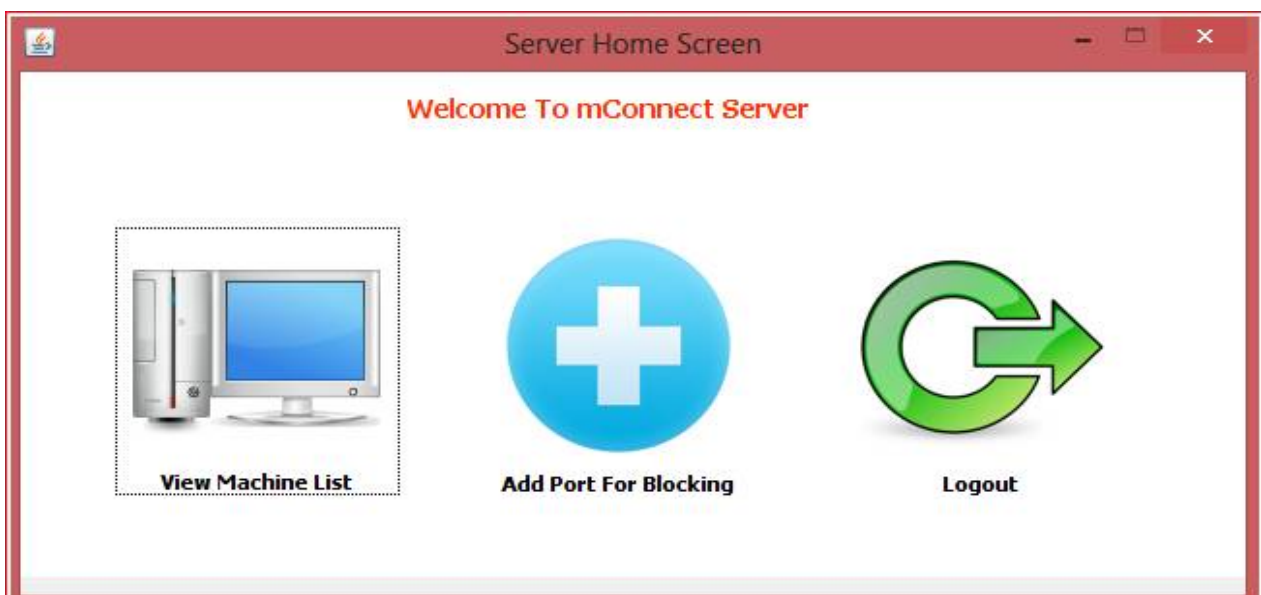


Fig 8.Admin Home Screen



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

The screenshot shows a window titled 'View Machine List' with a close button in the top right corner. Inside the window, there is a button labeled 'View Machine List' and a table with the following data:

Machine ID	Host Name	IP Address	MAC Address	Added On	Allow/Deny Status	Blocked Port
1	VINOD-JAISWAL	192.168.0.115	B4-82-FE-BA-7A...	2013-05-07 17:...	Y	9988,9980,909...
11	TECHNOWINGS...	192.168.198.1	00-50-56-C0-00...	2013-05-15 17:...	Y	9984
9	TECHNOWINGS...	192.168.0.101	90-E6-BA-BA-38...	2013-05-18 17:...	Y	9987,9987
10	TECHNOWINGS...	192.168.0.108	20-CF-30-CC-03...	2013-05-19 18:...	Y	
12	LAKHAN-PC	192.168.0.124	8C-A9-82-66-88...	2013-05-28 10:...	Y	
13	A	127.0.0.1		2015-03-22 18:...	N	

Below the table, there are four buttons: 'Allow Machine Access', 'Deny Machine Access', 'Machine Wise Block Port', and 'Refresh'.

Fig 9. View Machine Details

V. CONCLUSION AND FUTURE WORK

It is very easy to set up a successful rogue AP, this will result in major security problem. We have existing techniques for detecting rogue AP, but that technique has certain kinds of limitation. Disadvantage of manual Radio Frequency is that. RF scanning requires more time and it is tedious, which Detect rogue AP only, when scanning is applied. RF scanning method is also do impact on the costing and also it is not so effective and accurate. Automatic scanning depend on signs of APs (viz. MAC address, SSID, etc.) which is ineffective when a rogue AP spoofs signatures. We have mainly focused on identifying wireless vulnerabilities and security threats for the end users and finding solution to combat them.

REFERENCES

- [1]Prof..Dr.P.B.Mane “Illegal Access Point Detection Using Clock Skews Method in Wireless LAN”.
- [2]Amran Ahmad, Suhaidi Hassan ” Detecting Rogue Access Point (RAP) using Simple Network Management Protocol (SNMP) “ College of Arts and Sciences.
- [3]V. S. Shankar Sriram1, G.Sahoo3 “Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology” Department of Information Technology, Birla Institute of Technology, Mesra, Ranchi, India sriram@bitmesra.ac.in1 , drgsahoo@yahoo.com3
- [4] Liran Ma, Amin Y. Teymorian, Xiuzhen Cheng “A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi networks ”Department of Computer Science The George Washington University.

BIOGRAPHY

Amol Papade, Vikas Pansare and Rohit Patilare BE Students and **Prof.Swati Gore** theAssistant Professor in the Computer Engineering Department, Jaihind College of Engineering(Pune), SavitribaiPhule,Pune.