International Journal of Sciences: Basic and Applied Research (IJSBAR)

ISSN 2307-4531

http://gssrr.org/index.php?journal=JournalOfBasicAndApplied

Detecting And Eliminating Rogue Access Points In Ieee-802.11 Wlan - A Multi-Agent Sourcing Methodology

[*a]Priyanka G. Sasane, [b]S. K.Pathan

Pune University Smt. Kashibai Navale College of Engineering,
pdpatil.it@gmail.com

Abstract

For the Wireless Networks, presence of unapproved access points is becoming the major security issue. If this kind of network threats are not detected and mitigated on time, those will lead to the serious network damage and data loss. There are many researchers proposed solutions to overcome this security problem of WLAN, but those proposed tools having limitations or maybe they not automated to adopt the frequent changes in WLAN. We are into this research to present the new approach based on Master and Slave agents. This proposed approach not only looking for fast detection of Rogue Access points in the network but also presenting the solution to mitigate the WLAN from them. In short new framework is dealing with detecting as well as eliminating the Rough Access Points in the network. In proposed approach, the Master and slave agents are automatically scanning the networks for any unauthorized access points using the skew intervals. This Methodology has the following outstanding properties: (1) it doesn't require any specialized hardware; (2) the proposed algorithm detects and completely eliminates the RAPs from network; (3) it provides a cost-effective solution; (4) due to multiple master agents possibility of network congestion or delays is reduced. The proposed technique can block RAPs as well as remove them from the networks both in form of Unauthorized APs or as a Rogue Clients Acting as APs.

Keywords*:* Wireless LAN, Rogue Access point, Mobile agent, wireless network security, fake access point, time stamp.

1. INTRODUCTION

Communication over Wireless LANs System (WLANs) is one of the fastest growing technologies. The demand for connecting devices without use of cable has increased everywhere. Wireless networks are being driven by the need for providing network access to mobile or nomadic computing devices. Many of such benefits of mobility, greater flexibility, portability and freedom of access come with significant security and performance requirements.

One of the most challenging securities concerned for network administrator among all is the prevalence of Rogue Access Points (RAPs) [10- 12]. The reason why it's the most challenging is that nearly all of the other security threats either require a very high-level of technical knowledge or very sophisticated & costly intrusion devices, but these types of devices supporting RAPs could be easily accomplished by people with limited security backgrounds. Moreover, commodity Wi-Fi network cards that have the capability to capture all 802.11 transmissions can currently be purchased for about US $30 on eBay [5].

---

* Corresponding author.
E-mail address: pdpatil.it@gmail.com

A Rogue Access Point is typically referred to as an unauthorized AP in the literature. It is a wireless access point that has either been installed on a secure network without explicit authorization from a local administrator [15], or has been created to 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 present on about 20% of all enterprise networks [5]. Often these "Rogue" APs might be installed by valid user attempting to increase the range of the network but doing so without proper authorization. This usually results in a security hole that 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 -2].

There are various different classes of Rogue APs like unauthorized, improperly configured, phishing and compromised APs and related possible scenarios, readers are advised to refer [5] for detailed taxonomy. Although there are many commercial products of detecting RAPs are available on the market [10-12], there is still very less specific research work is been performed and published on RAP detection and even less on its complete elimination/blocking. In this paper, we propose a novel approach for not only its detection but also its elimination based on very new concept of Multi-Agent Sourcing Methodology.

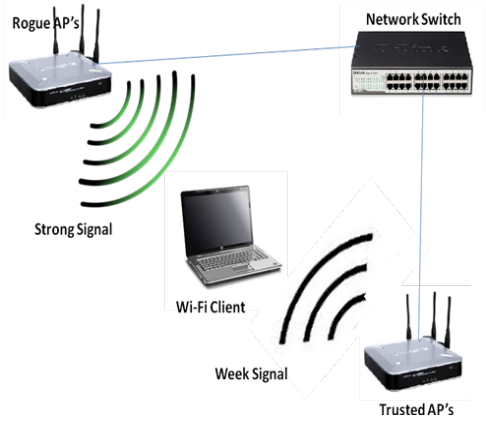

Fig 1: RAP's Higher Broadcast Power than Normal AP's

1.1 Motivation

Here we propose a fully automated concept (without any manual intervention) of detecting and eliminating RAPs by applying the mobile Multi-Agents onto the network. We are using two different levels of mobile agents-Master and Slave Mobile Agents. We extended the System Architecture as discussed in [1] in order to achieve a multi-agent sourcing methodology.

Initially a master agent is generated on the DHCP-M server, which is responsible for regulating all the authorization processes of the Wireless Network. This Master Agent generates slave agents depends upon the number of active Access Points Connected to the Server at that moment of time. These slave agents are then dispatched on the respective APs connected. Now these slave agents are cloned on every Access Points are being dispatched to the every connect client system to the APs. When the cloned salve agent at the client system detects any new Access Point, it automatically builds and sends a information packet INFO (SSID, MAC-Address, Vendors Name, Channel Used) of the Unauthorized AP to Clone Agent to the connected AP. The Slave Agent at AP dispatches this Information to its Master Agent on the Server. At the server the details of the suspected AP is detected and matched with that of the information stored into the repository about all the access points.

If the information is matched and the AP is found authorized then a new slave agent is generated and send to that AP, rather if it's detected as a client MAC address, a disassociation frame is send to all APs to inform them not to connect with it, else if the Details doesn't match with the either of it then the MAC-Address of the AP is fetched

from the INFO, the port at which the MAC-Address is connected is searched and then be blocked for any LAN traffic [Fig-2].

This would then automatically deactivate the RAP from performing any network activity on the Wireless Network. And also prevent the clients (if any) connected to the AP from dropping the connection and get associated to the nearest AP which is authorized. This is a very simple and most effective technique for completely routing out the Rogue Access Points from the network.

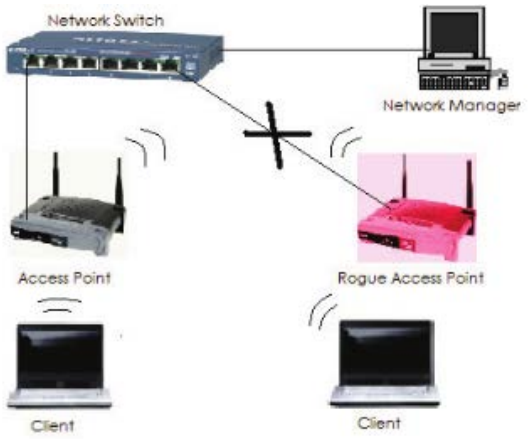

Fig 2: RAP's Higher Broadcast Power than Normal AP's

1.2 Problem definition

There are few researches already performed in this field, to detect and block the Rogue Access Points, but none of them is comprehensive. Most of them need to have a dedicated piece of software or hardware, or even some special qualified employees for performing different scans, or even some additional burden is given to the current employee for regular scanning of their vicinity for checking any unauthorized access points actively working around them.

2. Related work

Mobile Ad-hoc Networks (MANETs) are characterized by their lack of a fixed support infrastructure and their transient nature. Together, these characteristics lead to a very challenging environment for IDS implementation. Frequent changes in topology and communication patterns in MANETs require the use of specialized protocols and strategies for routing, transport and security.

The security research in MANET focused on key management, routing protocol and intrusion detection system, but past experiments have shown that encryption and authentication as intrusion prevention are not sufficient, and that more complex systems lead to more security problems.

On the other hand, intrusion detection techniques used in wired networks cannot be directly applied to mobile Ad Hoc networks due to special characteristics of the networks. Furthermore, most current MANET intrusion detection systems are still in the test stage. Thus, to limit the damages caused by attacks and make the ad hoc network more secure, there is a need for intelligent intrusion detection systems.

Intrusion detection techniques deployed for wired networks cannot be easily applied in wireless ad hoc networks due to the differences between these two types of networks. Compared to wired networks where traffic monitoring is performed in gateways, routers and switches, wireless ad hoc network lack traffic management points. As a result, intrusion detection in wireless networks should be based on local audit data. Moreover, because of the resource constraints that wireless networks present, one should focus on security mechanisms keeping in mind their resource

consumption characteristics. This means that it is better to use a periodic intrusion detection system (IDS) than an 'always-on' prevention mechanism.

The resource constraints that ad hoc networks face include limited battery, bandwidth and frequent miscommunication. These constraints complicate the discrimination between a new qualified operation after a disconnection and an intrusion. Another serious constraint that wireless ad hoc networks present is the difficulty of classification between normal and anomaly behavior.

As Discussed above, the security threats by a Rogue Access Point can de posed once connected to a network, and causes adversaries for committing espionage and launching attacks on a corporate Wi-Fi network. Detecting such APs is one of the most important tasks.

There are a variety of solution exists for detecting and eliminating Rogue Access Points. These solutions range from small, handheld devices to large installations of network hardware and software, but all of them offer incomplete solution.

2.1 Introduction to Mobile Agents

Mobile agents (MA) are software entities that can physically travel across a network, and perform tasks on machines that provide agent hosting capability. This allows processes to migrate from computer to computer, or processes to split into multiple instances that execute on different machines, and to return to their point of origin, which we will call the home context. Further, we will call the final node to visit by a mobile agent as its destination context. Migration of Mobile agent essentially implies that some code with required data is transferred to another node for remote execution.

Mobile agent is the software program that migrates from one host to another by themselves and interacts with other agents or distributed resources in the heterogeneous network. Plentiful study has proved that mobile agent has significant advantages, such as overcoming the network delay, reducing the payload in the intrusion detection field. Therefore, Mobile agent is wildly used in the intrusion detection study.

2.2 Advancement in the project

There are few researches already performed in this field, to detect and block the Rogue Access Points, but none of them is comprehensive. Most of them need to have a dedicated piece of software or hardware, or even some special qualified employees for performing different scans, or even some additional burden is given to the current employee for regular scanning of their vicinity for checking any unauthorized access points actively working around them.

We propose a fully automated concept (without any manual intervention) of detecting and eliminating RAPs by applying the mobile Multi-Agents onto the network. We are using two different levels of mobile agents- Master and Slave Mobile Agents.

3. System architecture

Our proposed architecture [Fig 3] uses a Mobile agent server which is also the DHCP server used for allocating IP address.

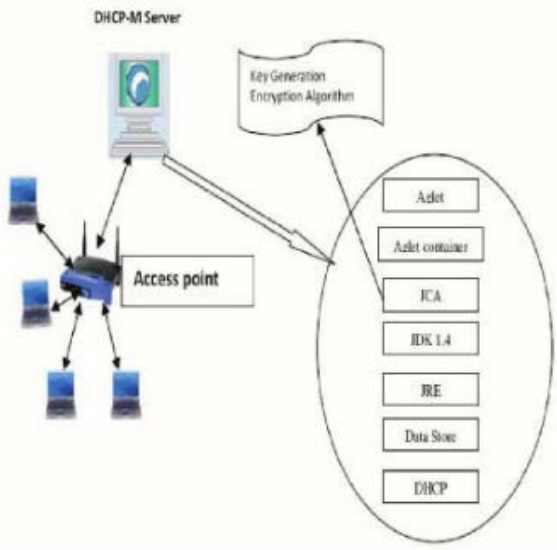

Fig 3: The system Architecture

3.1 Proposed Architecture

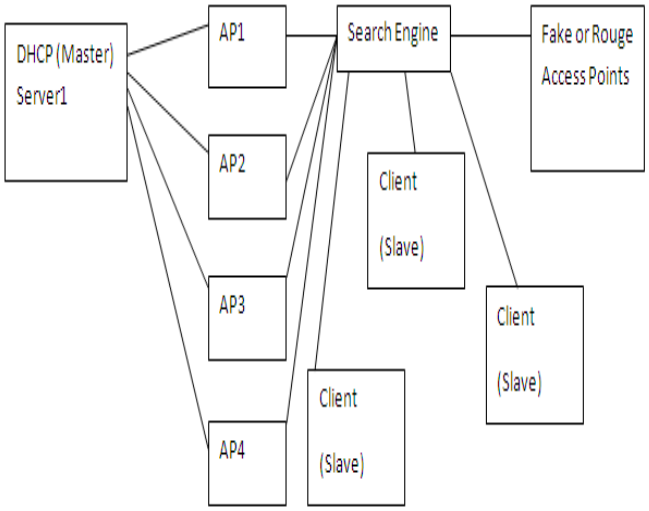

Fig 4: The system Architecture

Here we can include the concept of multiple servers so that if one server crashes down we can use another server to interact with the clients.

3.2 Use of Clock Skews

We explore the use of clock skew of a wireless local area network access point (AP) as its fingerprint to detect unauthorized APs quickly and accurately. The main goal behind using clock skews is to overcome one of the major limitations of existing solutions—the inability to effectively detect Medium Access Control (MAC) addresses spoofing. We calculate the clock skew of an AP from the IEEE 802.11 Time synchronization Function (TSF) time stamps sent out in the beacon/probe response frames. We use two different methods for this purpose—one based on linear programming and the other based on least-square fit. We supplement these methods with a heuristic for differentiating original packets from those sent by the fake APs. We collect TSF time stamp data from several APs in three different residential settings. Using our measurement data as well as data obtained from a large conference setting, we find that clock skews remain consistent over time for the same AP but vary significantly across APs. Furthermore, we improve the resolution of

received time stamp of the frames and show that with this enhancement, our methodology can find clock skews very quickly, using 50-100 packets in most of the cases.

4. Conclusion:

In this paper, we proposed a new methodology of using Multi- Agent as an integrated solution for both detecting and eliminating the Rogue Access Points from the network. Clear and easy to implement algorithm makes this architecture robust. This multi agent based architecture proved to not only identify but also eliminate the rogue access points completely. Our proposed technique is very reliable and cost effective, as it deals with multiple level of detection and doesn't require any specialized hardware device; implementation performed also supports our belief and results in a very effective methodology of complete removal of RAPs.

5. 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 (IACC 2009) Patiala, India, 6-7 March 2009.

[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] Manage Engine White Paper: Wireless Network Rogue Access Point Detection & Blocking

[10] "AirDefense enterprise: a wireless intrusion prevention system." [Online] Available: http://www.airdefense.net/

[11]"AirMagnet:EnterpriseWLANmanagement."[Online] Available: http://www.airmagnet.com/

[12] "Airwave: Wireless network management." [Online] Available: http://www.airwave.com/

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

[14] Sachin Shetty, Min Song, Liran Ma "Rogue Access Point Detection by Analyzing Network Traffic Characteristics" 1-4244-1513-06/07/$25.00 ©2007 IEEE.

[15] Raheem Beyah, Shantanu Kangude, George Yu, Brian Strickland, and John Copeland "Rogue Access Point Detection using Temporal Traffic Characteristics" published at IEEE Communications Society Globecom 2004

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

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