Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Investigation: Elimination of Fake Access Points from WLAN Using Skew Intervals

Mr. Ahmed Ayad Abdalhameed,
Assistant Lecturer, College Of Medicine,
University Of Baghdad, Iraq.

Abstract— The major security thread for the Wireless Networks is a presence of Rough access points. If this kind of network threats are not detected and mitigated on time, those will lead to the serious network damage and data loss. The use of clock skews of a wireless local area network access point (AP) as its fingerprint to detect unauthorized APs quickly and accurately we explore. Clock skews is to overcome one of the major limitations of existing solutions the inability to effectively detect Medium Access Control (MAC) addresses spoofing this is main goal behind using. For this purpose we use two different methods one based on linear programming and the other based on least-square fit. We are collecting TSF time stamp data from several APs in three different residential settings. In short new frameworks is dealing with detecting as well as eliminating the Rough Access Points in the network. 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 supplement these methods with a heuristic for differentiating original packets from those sent by the fake APs. In proposed system, the Master and slave agents are scanning the networks for any unauthorized access points using the skew intervals automatically. Basically during the paper we are investigating the very recent approaches presented for elimination of fake access points from the wireless networks efficiently.

Keywords— Wireless Security, WLAN, Rough Access Point, Master Agent, Slave Agent, DHCP.

I. INTRODUCTION

In Wireless LAN, most promising security concern is the presence of Rough access points which is also called as rogue access points [6]. The main 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 intrusion devices are very costly, but these types of devices supporting RAPs could be easily accomplished by people with limited security backgrounds. In Rogue Access Point typically referred to as an unauthorized AP in the literature. In 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.

The WLAN communication and data sharing is growing approach rapidly. Connecting with devices anywhere in the network it is anywhere demanded. Most of such benefits of mobility, higher flexibility, portability and freedom of access come with significant security and performance requirements. In wireless networks are being driven by the need for providing network access to mobile or nomadic computing devices. Wireless network communication imposes the new or more possibilities for network security threat and eavesdropping. Signals from wireless networks are usually unidirectional and emanate beyond the intended coverage area. Anyone with an appropriate wireless receiver can eavesdrop, and this kind of eavesdropping is virtually undetected. These properties make the physical security of the network mostly impractical.

Most of research paper discuss about the most common security protocol, Wired Equivalent Privacy (WEP), showing to be breakable even when correctly configured. Gartner research, we can claim that 20% of Wireless LAN word wide having Rough access points. There are 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. These "Rogue" Access Points might be installed by valid user attempting to increase the range of the network. There are different classes of Rogue APs like unauthorized, improperly configured, phishing and compromised Access Points and related possible scenarios. There are most of commercial products of detecting RAPs are available in market [6-8], there is still very less specific research work is been performed and published on Rough detection and even less on its complete elimination blocking. The various algorithms are investigated here for the elimination of fake access point from the network. In addition to this we have done the performance evaluation study between these two algorithms invested here.

II. INVESTIGATED ALGORITHM 1

Latest research on detecting and eliminating the rough access point based master and slave agents given below along with its limitation. This algorithm you can find in the [1] [2].

Proposed Approach Features:

1. No need any specialized hardware in any manner.
2. Includes both detection as well as prevention of RAP's from wireless networks.
3. Solutions are cost effective.
4. Use of Mobile agents in order to detect the RAP's.
5. Multi Agent approach.

Major Components of System:

-DHCP-M: This is central repository which is responsible for monitoring the authentication process of active wireless networks.
-Master Agent: Generated at DHCP Server.
-Slave Agent: Generated at every access point in network
-Clone Agent: Resided at client side.
-Access Point: Connected with DHCP sever
-Client: Connected with AP.

Latest Algorithm Steps:

- Generation of Master agent at DHCP Sever or repository.
- Generation of Slave Agent by master agents.
- Dispatching slave agents to all access points.
- Clone of slave agents created at all access points.
- On detection of new access point in the network by client, clone agent at client side build automatically INFO packet and send it to related slave agent.
- Slave agent forwards it to Master Agent.
- Master Agent forwards it to DHCP server for authentication.
- Various conditions checked for matching. If matches, then new slave agent generated for that new access point by Master Agent, else it is detected as rough access point.
- If it's not match, then following steps are taken to block that fake access point.
    1. Extract the MAC address from INFO packet.
    2. Extract the network switch address based on that extract MAC address
    3. Extract the connected port number based on MAC and Switch address.
    4. Finally block that port number from any other wireless LAN traffic.

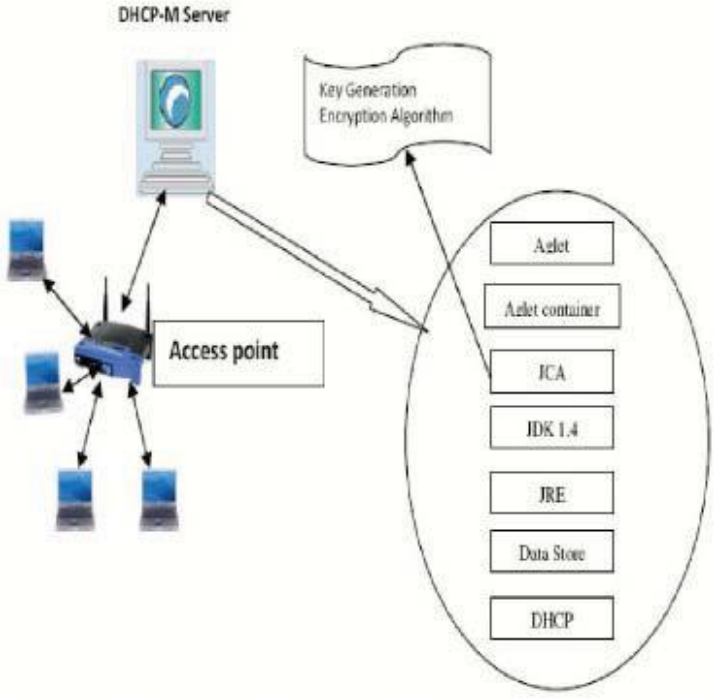

Figure 1: Architecture of Approach Proposed [1]

In above figure 1 shows the recent paper based proposed approach. Now we have following points which will be the limitation for this work:

- Due to the multi-agent system performance of proposed system and overall network may be down. Performance like overall throughput of wireless networks, packet drop ratio, end to end delay etc.

Heavy load on one master agent may take unnecessarily extra time while authenticating the new access point in the network, and hence this will may increase extra network overhead and decrease the network throughput.

III. INVESTIGATED ALGORITHM 2

In the recent paper [2], we have found below algorithm which is proposed to overcome above stated limitations of proposed algorithm 1. In this approach authors has find ways to verify and rectify the performance related issues:

1) Measurement by Performance: There are following measurements
   - Find out the throughput, delay end to end, ratio of network load etc. when the wireless network operating at normal mode.
   - Finding out the throughput, end to end delay, network load ratio etc when new access point is discovered by client or rough access point detection process.
   - Performance comparison between normal mode network and presence of rough access point detection and avoidance process.
2) Multiple Master Agents generation: We have to generate automatically two master agents, and if the access points are more means more than 10, it will generates the third master agent for the same. This will be the completely automated process. Here we are using the completely distributed architecture. If any master agent loaded gets with incoming traffic, then automatic handover is done to the master agent which is idle or having less traffic by discovering the network. Following figure shows the complete architecture for this approach.
3) Intervals Skew: This approach is used to continuously updating the master and slave agents for scanning the Rough access points.

Performance of this approach compared with performance of previous approach under the similar network conditions. Following figure 2 showing the architecture of new approach:

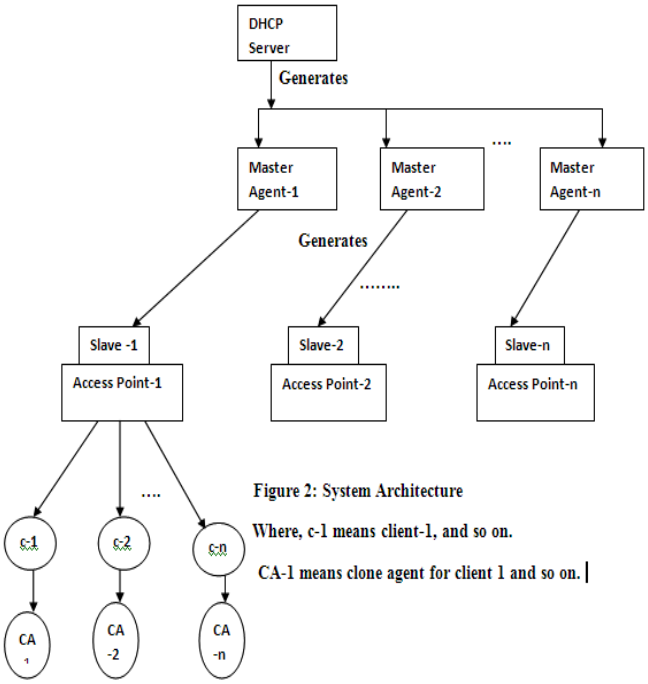

Figure 2: Algorithm 2, system architecture.

IV. WORK DONE

As we seen in the [2], the practical evaluation is done by author using the following terms. Main aim of the application is to detect the fake access points that are present in the network. These concepts used while developing this application is as follows:

Fake access point is a desktop application developed using c#.net. In this project author has developed an application in which the access points which provides data through internet are checked. If they are original or fake.

If they are fake then the access points are blocked for transferring data from our application.

In this application the modules presented was:

1. Detection of access points.
2. Checking of access point. Fake/original
3. Blocking the access point from transferring data.

The first module needs wifi connection and access points in our area to be detected. (Laptop has the wifi we can use it.). Using the WIFI and network we detect the access points which are providing the data to use.

In second module checking of the data obtained by the detected access point like MAC address, SSID, RSSI etc is done. Later based on these values the calculation of the skew interval for access point is done. And also estimate second skew interval from some equation and check for equality if they are same then access point will be original otherwise fake.

In this final module, they blocked the data coming from that access point which is faked. The port number of fake

access point was blocked. This port number is calculated from MAC address of that access point.

For performance evaluation the graphs calculation is done. The time graph as well as channel graph for each access point. Also filtering mechanism for filter the access point according to age, channel number etc. Below we are presenting the results presented in [2].

Result: Following are snapshots showing the framework with proposed approach:

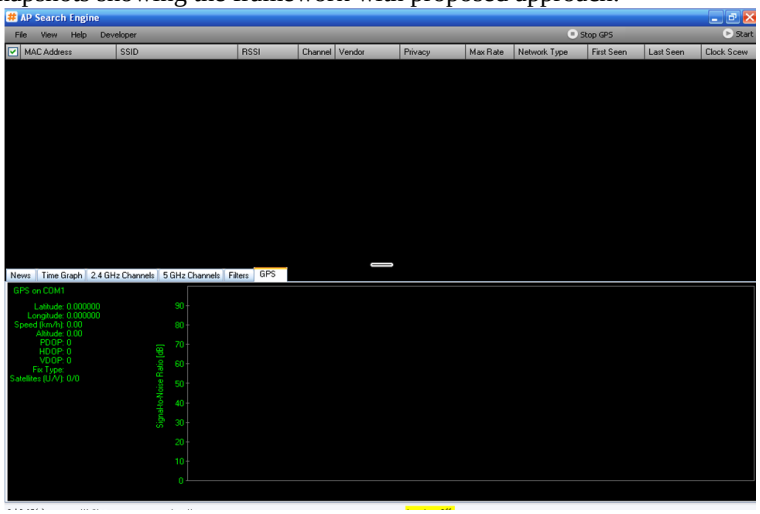

Figure 3: Main Screen for Proposed Framework

Above figure showing that your access point scanning windows is ready to capture all the available access points' networks in your area.

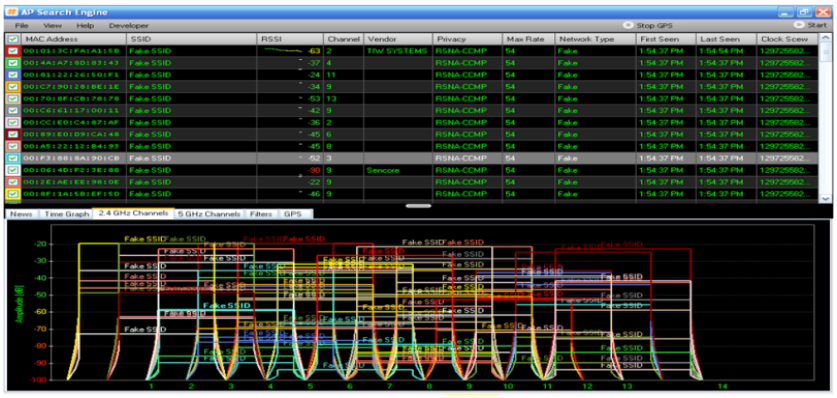

Figure 4: Results after detecting Rough AP.

Above figure 4 is showing the graphical performance of network after detecting the Rough access point in the wireless network.

Following figure showing the filters settings for skew used in order to perform the efficient working of framework.

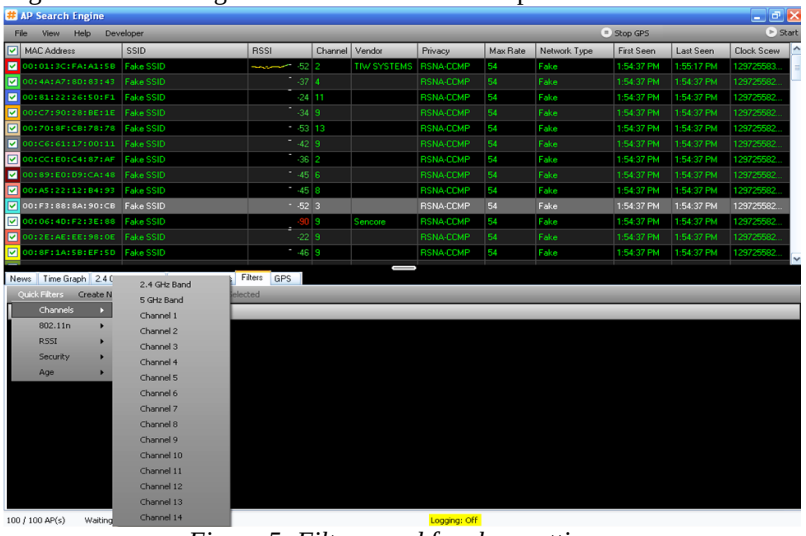

Figure 5: Filters used for skew settings.

From these results, I have concluded with following performance evaluation graphs:

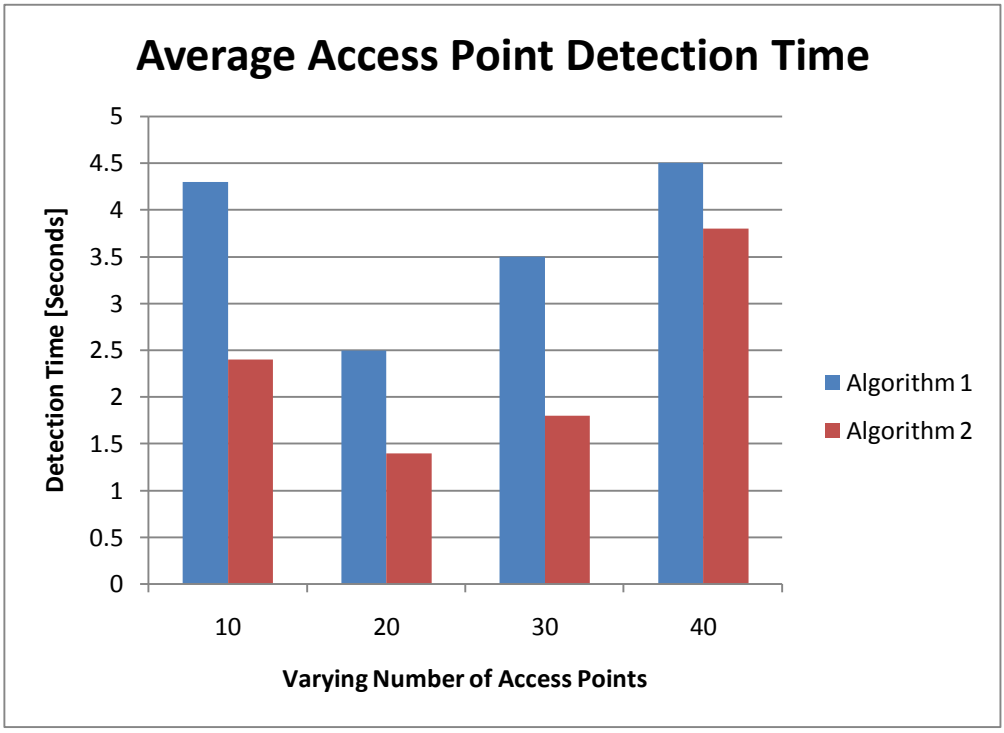

Figure 6: Performance Comparison of Detection of Access point time.

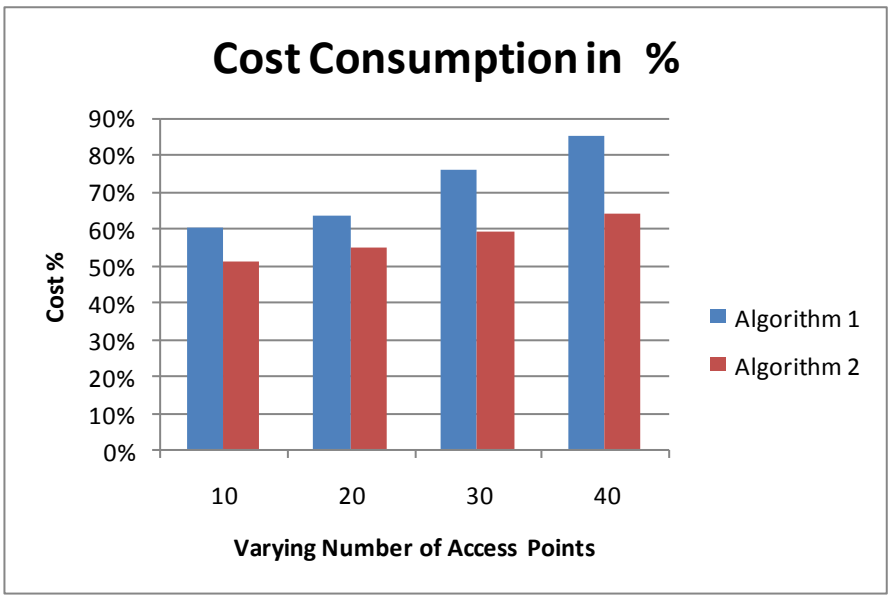

Figure 7: Performance Comparison of Cost Consumption in %

This above graphs of analysis showing that the second proposed algorithm is having better performances as compared to algorithm 1. Hence we claim that proposed approach presented in [2] is overcoming the limitations of proposed approach presented in [1].

V. CONCLUSIONS

During this paper, our main aim was to investigate and analyze the best efficient method for the detection and prevention of fake access points from the wireless sensor networks. We have studied two algorithms and presented their working methods. In the second proposed system new methodology of using Multi- Agent as an integrated solution for both eliminating & detecting the Rogue Access Points from the network. This multi agent based architecture proved to not only identify but also eliminate the rogue access points completely Easy to implement algorithm makes this architecture robust. Our proposed system is very cost effective & reliable, as it deals with multiple level of detection and doesn't require.

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] Prof.S.B.Vanjale (Ph.D Student), J.A.Dave(M.Tech. Student), "Unapproved Access Point Elimination In Wlan Using Multiple Agents And Skew Intervals", Department of Computer Engg Bharati Vidyapeeth Deemed University College of Engineering Pune, International Journal of Engineering Science and Technology (IJEST), Feb. 2012.

[3] 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.

[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

