Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN Based on Agents Terminology and Skew Intervals: A Proposal

Ahmed Ayad Abdalhameed

Abstract- The existence of rough access points in the network is now days becoming very serious security threat for networks line WLAN. The presence of such network threats always resulted into the important information leakage or damage. Previously already many tools are developed by different research groups, however they are coming with some limitations which we have to discuss and address in this research proposal. Here the agent based approach is present not only to detect the rough access points but also their elimination from the wireless networks efficiently and with minimum cost involvement. The master agent and slave agents are generated automatically, which are acts as major components for providing the security to wireless networks. These agents are continuously doing the process of networks scanning to capture the rough access points and eliminate them. This scanning is scheduled based on clock skews which are playing important role. This Methodology has the following outstanding properties: (1) it doesn't require any specialized hardware; (2) the proposed algorithm detects and completely eliminates the UAPs 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 UAPs as well as remove them from the networks both in form of Unauthorized APs.

Index Terms—Fake Access Points, clock skews, master, slave, wireless networks.

I. 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. The wireless medium introduces new opportunities for eavesdropping on wireless data communication. Signals from wireless networks are usually unidirectional and emanate beyond the intended coverage area. Such properties make the physical security of the network mostly impractical. Anyone with an appropriate wireless receiver can eavesdrop, and this kind of eavesdropping is virtually undetected. Various research paper discuss about the most common security protocol, Wired Equivalent Privacy (WEP), has been shown to be breakable even when correctly configured.

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].

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.

We explore the use of skew interval of a wireless local area network access point (AP) as its fingerprint to detect unauthorized APs quickly and accurately. The main goal behind using skew intervals 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 skew interval 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 Unapproved 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 skew intervals 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 skew intervals very quickly, using 50-100 packets in most of the cases. We also discuss and quantify the impact of various external factors including temperature variation, virtualization, skew source selection, and NTP synchronization on skew intervals. Our results indicate that the use of skew intervals appears to be an efficient and robust method for detecting rough APs in wireless local area networks.

Manuscript published on 30 April 2013.
***** Correspondence Author (s)
Ahmed Ayad Abdalhameed, Assistant Professor, College Of Medicine,University Of Baghdad, Iraq.

II. PROPBLEM 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. The use of Wireless networks is more as compare to fixed networks now days, almost 70 % of network communications, transactions and billing is going through the wireless networks. However such wireless networks more vulnerable for the attacks like malicious attacks, selfish node attacks, and duplicated access points attacks in order to damage or leak the important information. This becomes the serious problem for wireless networks. There are many tools are already presented by researchers, but those are having limitations which we need to overcome in this research.

III. LITERATURE SURVE ON WLAN SECURITY

The broadcast properties of wireless technology make it vulnerable to a series of attacks. Snooping on a wireless network consists of using a laptop, a wireless card, and some software while being in transmission range of a wireless network. The service set identifier, or SSID is the name of the wireless network and it can be used to gain access. Turning off SSID broadcasting means that no one can see it by using an auto find of networks. However, if you leave the default SSID unchanged; a hacker could try the common SSIDs and connect to your network (assuming WEP is off). MAC address filtering can be used to increase the security of your network. It works by allowing only a set list of network cards to connect based upon their known MAC address, which should be unique for every device. However, MAC address can be captured but snooping and spoofed which will then allow an attacker to gain access. Most wireless cards now allow MAC addresses to be changed [6, 7].

The second type of attack utilizes vulnerabilities in the Wired Equivalent Privacy, or WEP, key. The WEP key utilizes an RC4 encryption algorithm, also known as a stream cipher. The sender takes a key and expands it to a lengthy random key stream and then XORs that with the information that is being sent. The receiver also has the same key and XORs the cipher-text, which gives the original information. This presents a problem because when an attacker has obtained two cipher-texts encrypted with the same WEP key, he can then XOR the two together and get the original information without needing to decrypt it with the WEP.

To prevent against this, an integrity check is implemented using an Initialization Vector, or IV. This vector prevents the same random key stream from encrypting two different packets. Unfortunately, it is only 24 bits long, which means that a busy access point will have to reuse the same random key stream sometime, usually within a few hours. An attacker will still be able to sniff this information off the network and use XOR to obtain the original information.

WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. For RC4, WEP uses two key sizes: 40 bit and 104-bit; to each is added a 24-bit initialization vector (IV) which is transmitted in the clear. Cam-Winget et al. (2003) surveyed a variety of shortcomings in WEP. Two generic weaknesses were that: § the use of WEP was optional, resulting in many installations never even activating it, and § WEP did not include a key management protocol, relying instead on a single shared key amongst users.

More specific attacks have also become evident: in August 2001, Fluhrer et al. published a cryptanalysis of WEP that exploits the way the RC4 cipher is used, resulting in a passive attack that can recover the RC4 key after eavesdropping on the network for a few hours; the attack was soon implemented, and automated tools have since been released. It is possible to perform the attack with a personal computer, off-the-shelf hardware and freely-available software. Cam-Winget et al. write, "Experiments in the field indicate that, with proper equipment, it is practical to eavesdrop on WEP-protected networks from distances of a mile or more from the target. In 2005, a group from the U.S. Federal Bureau of Investigation gave a demonstration where they broke a WEP-protected network in 3 minutes using publicly available tools. We will perform some of these attacks [6].

One of the most basic attacks a hacker can perform once finding a wireless network is to identify the access point, AP, and check to see if the default settings are in use. A large number of home users, and some businesses, do not change their settings on their AP. Once the brand of the device is known, its default settings are easy to lookup on the internet, as companies publish them so people can use their devices.

Encrypted Traffic

Data security in 802.11 is usually accomplished by Wireless Equivalent Privacy (WEP). The RC4 stream-cipher algorithm is used to encrypt the data. WEP relies on a secret key, normally 40 bits, and an initialization vector (IV), which is 24 bits, as a seed for the algorithm. The encryption of a frame proceeds as follows [8]:

RC4 generates a pseudorandom stream of bits (a "keystream") which, for encryption, is combined with the plaintext using XOR as with any Vernam cipher; decryption is performed the same way. To generate the keystream, the cipher makes use of a secret internal state which consists of two parts:

1. A permutation of all 256 possible bytes (denoted "S" below).
2. Two 8-bit index-pointers (denoted "i" and "j").

The permutation is initialised with a variable length key, typically between 40 and 256 bits, using the key-scheduling algorithm (KSA). Once this has been completed, the stream of bits is generated using the pseudo-random generation algorithm (PRGA).

For as much iteration as are needed, the PRGA modifies the state and outputs a byte of the keystream. In each iteration, the PRGA increments i, adds the value of S pointed to by i to j, exchanges the values of S[i] and S[j], and then outputs the value of S at the location S[i] + S[j] (modulo 256). Each value of S is swapped at least once every 256 iterations.

```
i := 0
j := 0
```

```
while Generating Output:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap(S[i],S[j])
    output S[(S[i] + S[j]) mod 256]
```

The key-scheduling algorithm is used to initialise the permutation in the array "S". "l" is defined as the number of bytes in the key and can be in the range 1 ≤ l ≤ 256, typically between 5 and 16, corresponding to a key length of 40–128 bits. First, the array "S" is initialised to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA algorithm, but also mixes in bytes of the key at the same time.

```
for i from 0 to 255
    S[i]:= i
 j := 0
 for i from 0 to 255
    j := (j + S[i] + key[i mod l]) mod 256
    swap(S[i],S[j])
```

RC4 falls short of the standards set by cryptographers for a secure cipher in several ways, and thus is not recommended for use in new applications.

The keystream generated by RC4 is slightly biased in favour of certain sequences of bytes. The best attack based on this bias is due to Fluhrer and McGrew, which will distinguish the keystream from a random stream given a gigabyte of output.

RC4 does not take a separate nonce alongside the key. As with any cipher, but particularly with Vernam ciphers, such a nonce is a requirement for security, so that encrypting the same message twice produces a different ciphertext each time. A secure solution to this that works for any secure cipher is to generate each RC4 key by hashing a long-term key with a unique nonce using a construction such as HMAC. However, many applications that use RC4 simply concatenate key and nonce; RC4's weak key schedule then gives rise to a variety of serious problems.

In 2001 a new and surprising discovery was made by Fluhrer, Mantin and Shamir: over all possible RC4 keys, the statistics for the first few bytes of output keystream are strongly non-random, leaking information about the key. If the long-term key and nonce are simply concatenated to generate the RC4 key, this long-term key can be discovered by analysing large number of messages encrypted with this key. This and related effects were then used to break the WEP ("wired equivalent privacy") encryption used with 802.11 wireless networks. This caused a scramble for a standards-based replacement for WEP in the 802.11 market, and led to the IEEE 802.11i effort and WPA. Cryptosystems can defend against this attack by discarding the initial portion of the keystream (say the first 1024 bytes) before using it [9].

While WEP may sound like a great idea, it is inherently flawed on many levels. For the scope of this lab, the major flaws lie in the use of the initialization vector and the RC4 algorithm itself. In a paper entitled Weaknesses in the Key Scheduling Algorithm of RC4 by Fluhrer, Mantin, and Shamir, the authors propose a method in which under certain conditions the key setup algorithm of RC4 can leak information about the secret key. To attack RC4, they propose to search for specific IV’s that place the keystream in this vulnerable state. In the parlance of this attack, these vectors are called “interesting”. By collecting enough of these “interesting packets” the entire secret key can be reconstructed.

Since the summer of 2001, WEP cracking has been a trivial but time consuming process. A few tools, AirSnort perhaps the most famous, that implement the Fluhrer-Mantin-Shamir (FMS) attack were released to the security community -- who until then were aware of the problems with WEP but did not have practical penetration testing tools. Although simple to use, these tools require a very large number of packets to be gathered before being able to crack a WEP key. The AirSnort web site estimates the total number of packets at five to ten million, but the number actually required may be higher than you think.

The first caveat to this old approach is that only encrypted packets count. As wireless access points transmit unencrypted beacons several times per second, it is easy to be fooled into believing that you have a larger number of useful packets than you really do. If you use Kismet for network discovery and sniffing, it breaks down the packet count for you, displaying the number of "Crypted" packets separately from the total number.

The second thing working against your packet collection efforts is that only certain "interesting" or "weak" IVs are vulnerable to attack. Kismet also tells you how many of these have been gathered, although it may not use the same counting method as the various cracking tools. To make matters more difficult, wireless manufacturers responded to the FMS attack by filtering out the majority of weak IVs that their access points and wireless cards transmit. Unless your target network is using old equipment, chances are you'll have to collect no less than ten million encrypted packets to crack a WEP key using these older tools.

On August 8th, 2004, a hacker named KoreK posted new WEP statistical cryptanalysis attack code (soon to become a tool called chopper) to the NetStumbler forums. While chopper is functional, it is not currently maintained, and the attacks have since seen better implementations in aircrack and WepLab. However, the KoreK attacks change everything. No longer are millions of packets required to crack a WEP key; no longer does the number of obviously "weak" or "interesting" IVs matter. With the new attacks, the critical ingredient is the total number of unique IVs captured, and a key can often be cracked with hundreds of thousands of packets, rather than millions [9].

IV. PROPOSED ALGORITHM

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 in order to achieve a multi-agent sourcing methodology with addition of skew intervals in order to periodically scan the networks.

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. 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. Below is the algorithm which is extended with insertion of skew intervals: This algorithm is based on components such as DHCP server, slave agent, master agent etc

- Master agent generation at server of DHCP.
- Slave Agents generation form the generated Master agent.
- Scanning all the access points and assigning slave agents to all of them one by one.
- Generation of slave agents clone at all the access points.
- Generation of clock skews at each slave agents in order to scan the access points.
- Once the new access point is scanned by salve agent, then slave agent building the packet of INFO to send over the master agent.
- This new INFO packet is sent over master agent who then forwards to the DHCP repository which is continuously looking for requests from master agent.
- The authentication of new access point is checked at DHCP server by matching process. If the match process is done successfully then new slave agent is created for new access point. Otherwise, new access point is detected as fake access point and then goes through below process for its elimination: Various conditions checked for matching. If matches,
- If it's not match, then following steps are taken to eliminate that fake access point.

1. The MAC address is extracted from the INFO packet of that new access point.
2. Extract the connected port number based on MAC and Switch address.
3. Extract the network switch address based on that extract MAC address
4. At last, block that port number from any other wireless LAN traffic.

V. PRACTICAL DESING

Following diagrams shows the practical design approach of this new method of detection and prevention of rough access points from wireless networks:

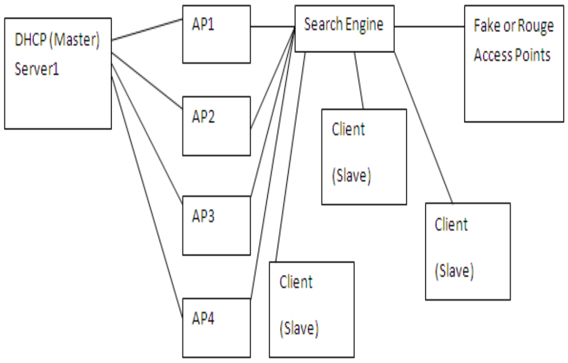

Figure 1: Proposed architecture design

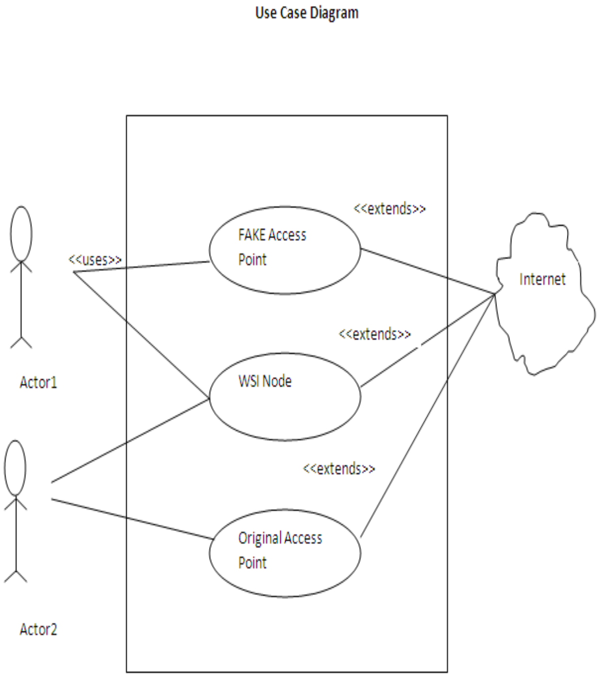

Figure 2: Use Case implementation design

VI. CONCLUSION

At first look, this approach look very efficient, however its efficiency will get evaluate during the practical experiments over real time wireless networks. Here I extended the approach of master and slave based mechanism to detect and prevent the fake access points from the wireless networks. In above proposed algorithm we added the concepts of clock skews which improves the performance and allows every slave agents to periodically scan not only new access points but also the existing access points for any unauthorized actions.

REFERENCE

[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