International Journal of Smart Sensor and Adhoc Network

Volume 1 | Issue 2 Article 16

2011

Detecting & Eliminating Rogue Access Point in IEEE 802.11 WLAN

S. B.Vanjal
Department of Computer Engg Bharati Vidyapeeth Deemed University College of Engineering Pune.,
svanjale@rediffmail.com

Amol K. Kadam
Department of Computer Engg Bharati Vidyapeeth Deemed University College of Engineering Pune.,
akkadam@bvucoep.edu.in

Pramod A. Jadhav
Department of Computer Engg Bharati Vidyapeeth Deemed University College of Engineering Pune.,
pramodjadhav1408@gmail.com

Detecting & Eliminating Rogue Access Point in IEEE 802.11 WLAN

S.B.Vanjale, Amol K. Kadam, Pramod A. Jadhav
Department of Computer Engg
Bharati Vidyapeeth Deemed University College of Engineering Pune.
svanjale@rediffmail.com, akkadam@bvucoep.edu.in, pramodjadhav1408@gmail.com

Abstract: Rogue Access Points (RAPs) is one of the leading security threats in current network scenario, if not properly handled in time could lead from minor network faults to serious network failure. Most of the current solutions to detect rogue access points are not automated and are dependent on a specific wireless technology. In this paper we propose the integrated solution for detection and eliminate the rogue access points.

Rogue detection algorithm is also proposed. This Methodology has the following properties: (1) it doesn't require any specialized hardware; (2) the proposed algorithm detects and completely eliminates the RAPs from network; Our proposed solution is effective and low cost.

Keywords: Rogue Access Points, Wireless Security, Mobile Agents, Wireless LANs.

1. INTRODUCTION

Currently many organizations utilize the wireless LAN to provide the access channel to the Internet and Intranet enabling the flexible workforce. Employees are able to move their computers from one location to another. While doing so, communications with peers and the Internet are continuously maintained. It has been clearly shown that utilizing wireless LAN helps increasing the productivity of a company that is using it. However the wireless security is always a primary concern. The information transmitted by the users is broadcasted through the air. Everybody within range of the wireless signal can easily tune in and capture the data. Most enterprise wireless implementations normally include the wireless security measure such as IEEE 802.11i or WPA (Wireless Protected Access). IEEE 802.11i provides the encryption and authentication mechanisms to protect user from unauthorized access and data eavesdrop over the wireless network. However, such security measures cannot protect the system from the unauthorized installation of the access point by their own staffs. The staffs can easily plug in the unauthorized access point (normally called rogue access point) to the network for their personal usage. Most staffs are unaware of the security threats that come along with this act. The unauthorized user or hacker can bypass the company's line of network defenses (i.e., firewall, access control) through the rogue access point and poses the serious threat to the organization.

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, 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.

Rogue APs are present on about 20% of all enterprise networks. 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.1).

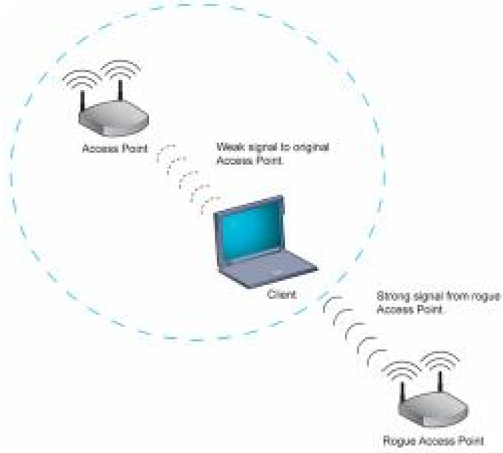

Access Point
Weak signal to original Access Point.
Client
Strong signal from rogue Access Point.
Rogue Access Point

Figure 1 RAPs Higher Broadcast Power than Normal APs.

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.

In our work, we designed and implemented a fully secured agent-based intrusion detection system that detects the presence of unauthorized wireless elements, namely, rogue access points, wireless promiscuous nodes and unauthorized clients. Depending on the kind of wireless element detected, the system would respond accordingly. In the case of the wireless element being a rogue access point or a wireless promiscuous node, the response would be sending the relevant information such as the geographical information, the time when the element was detected, etc. to the concerned personnel. If the wireless element turns out to be an unauthorized client, the response would be blocking that client from getting onto the network, thus preventing unauthorized access.

The Proposed Solution:

In this paper we propose the solution that is different from the previous works.

Key features are:1) The integrated rogue access point detection and eliminate 2) Use existing access point as the wireless sensor. No dedicated wireless sensor is required. The proposed system consists of 3 main components:

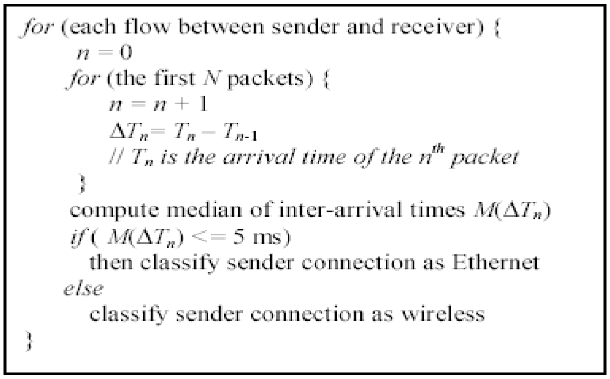
1) Access Point 2) Switch 3) Central System

2.THE CURRENT APPROACHES

Wireless Approach:-

Most of the current approaches for detecting rogue APs are rudimentary and easily evaded by hackers. Some organizations have equipped IT personnel with wireless packet analyzer algorithm fig-1, forcing IT personnel to walk the halls of the enterprise or campus searching for rogue APs. This method is generally ineffective because manual scans are time-consuming and expensive – and, therefore, are conducted infrequently. Also, with 802.11 hardware operating at separate frequencies (802.11a - 5Ghz and 802.11b - 2.4Ghz), IT personnel must upgrade their detection devices to accommodate multiple frequencies. Moreover, scans are easy to elude, since a rogue AP can easily be unplugged when the scan takes place.

Wireless Traffic Analyzer:-



```
for (each flow between sender and receiver) {
      $n = 0$
      for (the first $N$ packets) {
            $n = n + 1$
            $\Delta T_n = T_n - T_{n-1}$
            // $T_n$ is the arrival time of the $n^{th}$ packet
      }
      compute median of inter-arrival times $M(\Delta T_n)$
      if ( $M(\Delta T_n) <= 5$ ms)
         then classify sender connection as Ethernet
      else
         classify sender connection as wireless
}
```

Figure-2: Wireless traffic analyzer algorithm.

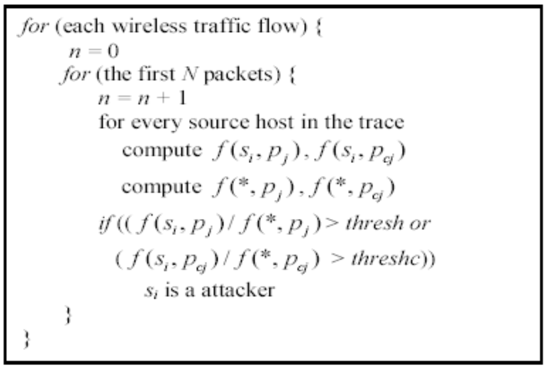
we propose the solution that is different from the previous works. Key features are: 1) The integrated rogue access point detection systems 2) Use existing access point as the wireless sensor. No dedicated wireless sensor is required. The proposed system (shown in Figure 2) consists of 3 main components: 1) Access Point: the access point can operate in two modes: **Normal Mode** is the mode that the access point performs as the regular access point and **Sniffer Mode** is the mode that the access point performs as the wireless sniffer collecting surround wireless data.

2.1 Rogue Access Point Detection

The rogue access point detection starts with RF sniffing to collect wireless data and then analyze the collected data to determine the rogue access point. The rogue access point sniffer phase has the processes as follows:

1) The access point is changed the mode from Normal Mode to Sniffer Mode and operates as wireless sniffer collecting wireless sniffing data including Beacon, Probe messages and client data frames. The frame format of wireless sniffer data is shown in Figure 3.

2) Wireless sniffing data will be normalized to remove irrelevant information out and stored the rest to the database.



```
for (each wireless traffic flow) {
    $n = 0$
    for (the first $N$ packets) {
        $n = n + 1$
        for every source host in the trace
            compute $f(s_i, p_j), f(s_i, p_{cj})$
            compute $f(*, p_j), f(*, p_{cj})$
        if(( $f(s_i, p_j) / f(*, p_j)$ ) > thresh or
            ( $f(s_i, p_{cj}) / f(*, p_{cj})$ ) > threshc))
            $s_i$ is a attacker
    }
}
```

Figure-3: Rogue access point detection algorithm

The potential rogue access point data is stored in the database waiting for analyzed. Central system analyzes the rogue access point based on the detection algorithm shown in Figure 2. The algorithms are the follows:

1) Compare the sniffing data (i.e., SSID, Wireless MAC) with the authorized AP information. The authorized AP information is stored before hand. There are three possible outcomes: Completely Matched (SSID and MAC), Completely Unmatched (not SSID and not MAC) and Partially Matched (not SSID but MAC, or SSID but not MAC). If Completely Matched, goto stage 2). If Partially Matched, goto stage 3) and If Completely Unmatched goto stage 4)

2) For Completely Matched, there are two possibilities of access points: *Trusted AP* or *Attacker Rogue AP*. The attacker rogue AP completely spoofs the authorized AP information (i.e., spoof MAC and spoof SSID). Typically it is hard to verify if an AP is the legitimate one. Therefore, we propose the technique that can differentiate Trust APs from Spoof Rogue AP using timestamp information within Beacon. Normally each access point will includes the timestamp on the Beacon. The timestamp is total uptime of the access point measured since its start. Even though the attackers can manipulate the spoof SSID and wireless MAC, they will have the difficult time trying to synchronize and spoof timestamp of the trusted AP.

3) For Partially Matched, the result would be either Misconfiguration AP or Attacker's Rogue AP. The Misconfiguration AP is the access point with configuration that is not consistent to the registered AP. Verifying the configuration of all APs will remove the outcome of Misconfiguration AP and leave remaining of Attacker's Rogue AP.

4) For Completely Unmatched, the result would be either Neighborhood AP or Employee rogue AP. If the AP connects to the external network, we can assume that it is Neighborhood AP. If the AP connects to the internal network, it is Employee rogue AP. The technique to perform "AP internal connection checking" or AP localization is described in the next section.

3.EXPRERIMENTAL RESULT

The experimental setup is shown in Figure 4. It consists of AP, Central Server, Manage AP, Rogue AP and Wireless Client.

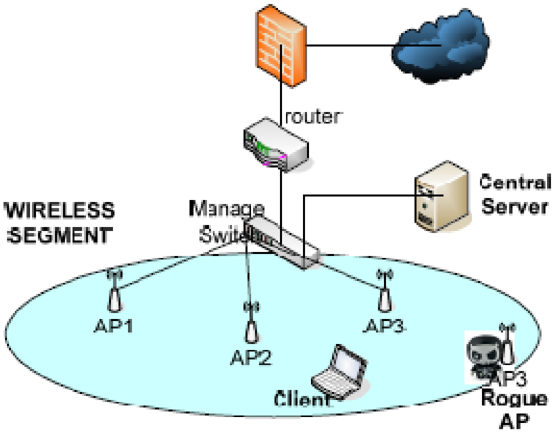


Figure- 4: Experimental Setup

The central server contains

1. Expect – the Expect is the software tool used to remotely control the AP mode switching through SSH.

2. Advance java for the web service

3. MySQL for the rogue access point database

3.1 Rogue Access Point Detection

In this section, we perform the experiment to show how the proposed system can detect the various types of rogue access point. We define four types rogue access point.

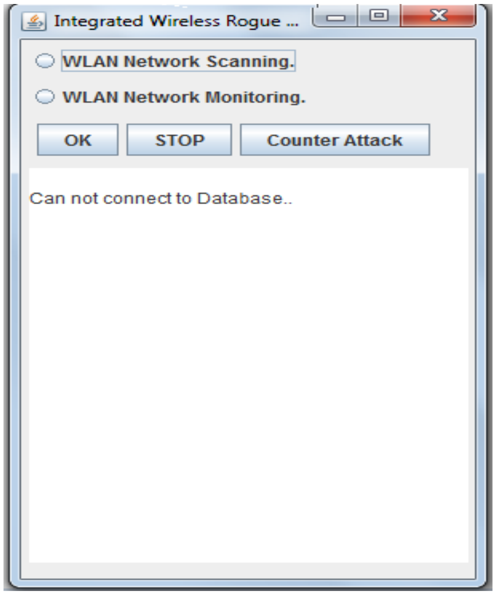
1. Rogue Type 1: Employee’s rogue access point, no SSID spoof and no wireless MAC spoof.

2. Rogue Type 2: Attacker’s rogue access point, with SSID spoof but no wireless MAC spoof

3. Rogue Type 3: Attacker’s rogue access point, with no SSID spoof but wireless MAC spoof.

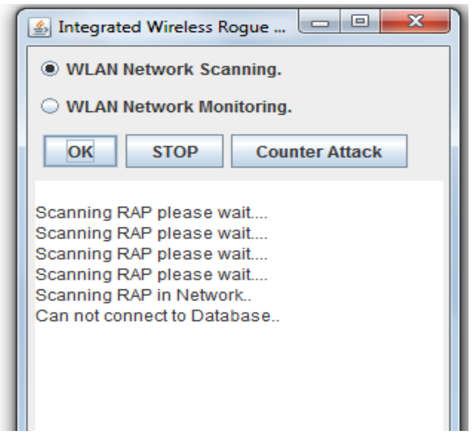
4. Rogue Type 4: Attacker’s rogue access point, with SSID spoof and wireless MAC spoof.

We set up the Authorized AP with SSID “RDS” and wireless MAC “0019e8d90ba0” and each type of rogue access point as shown in Table 2 (Note: the shade cell represents spoofing). The result (see Figure 6) shows our system can detect all four types rogue access point.



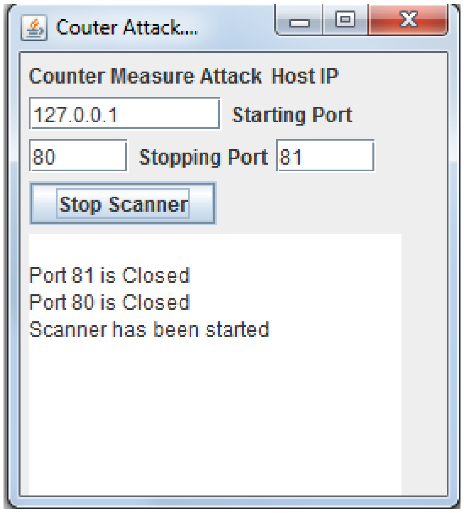
```
Can not connect to Database..
```

Figure- 5: Scanning Wireless Network.



```
Scanning RAP please wait....
Scanning RAP please wait....
Scanning RAP please wait....
Scanning RAP please wait....
Scanning RAP in Network..
Can not connect to Database..
```

Figure 6: Scanning RAP.



Counter Measure Attack Host IP: 127.0.0.1
Starting Port: 80
Stopping Port: 81

```
Port 81 is Closed
Port 80 is Closed
Scanner has been started
```

Fig 7: Counter Attacks.

4. SECURE WIRELESS SYSTEM

In order to mitigate the rogue access point effectively the secured wireless system is required. The recommendation of secured wireless system is summarized as the follows:

1) ***Wireless Security Policy*****:** Wireless Security Policy plays key role to guide the company to the right direction of secured wireless. Policy presents the commitment on the security issues. It should clearly state the important of security, unauthorized access point will not be allowed and also state the consequence of policy violation. Furthermore, there should be the regular announcement or reminder about the security policy to employees.

2) ***Wireless Risk Assessment:*** Annual wireless risk assessment is also essential. Wireless risk assessment analyzes the threat, vulnerability and the impact. Wireless risk assessment provides the priority of how importance we should protect our system.

3) ***Confidentiality*****:** the encryption will provide the secure communication over the wireless LAN. WPA or IEEE 802.11i is the common solution.

4) ***Physical Security*****:** To secure the physical access is important. All network equipments (such as server, access point and switches) should be securely protected from the unauthorized access. LAN outlet should also be secure.

5) ***Awareness Training and Education*****:** The employees are required to have the awareness training regularly.

5. CONCLUSION

In this paper we propose the Detecting & Eliminating the rogue access points. Classification of rogue access point and related risk assessment is analyzed. Rogue detection algorithm is also proposed. Our proposed solution is effective and low cost. It is designed to utilize the existing wireless LAN infrastructure. There is no need to acquire the new RF devices or dedicated wireless detection sensors. The experiments in the real system are demonstrated.

REFERENCES

Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology
V. S. Shankar Sriram1, G.Sahoo3
Department of Information Technology,
Birla Institute of Technology, Mesra, Ranchi, India
sriram@bitmesra.ac.in1 , drgsahoo@yahoo.com

Integrated Wireless Rogue Access Point Detection and Counterattack System
††Intelligent Wireless Network Group (IWING)
Department of Computer Engineering, Faculty of Engineering, Kasetsart University
50 Pahon-Yothin Rd., Cha-tuchak, Bangkok 10900, Thailand.
Tel: +66-2942-8555, Fax +66-2579-6245
songrit.srilasak@nectec.or.th

Agent Based Intrusion Detection and Response System for Wireless LANs
Mohan K Chirumamilla
Department of Computer Science and Engineering
University of Nebraska-Lincoln
Lincoln, NE, 68588-0115 U.S.A.
mohankc@cse.unl.edu