Analysis of security in wireless network: Result analysis

[1]Abhimanyu Dnyandeo Sangale, [2]Dr.Sanjeev Kumar Sharma

[1]Research Scholor, [2]Research Guide
Oriental University, Indore (MP)

***Abstract*: A novel techniques are introduced to detect rouge APs and to improve network resilience. Here an efficient rogue AP protection system termed as RAP for commodity Wi-Fi networks is proposed. This system should the following Properties: it requires neither specialized hardware nor modification to existing standards; the proposed mechanism can be integrated with an AP in a plug-in manner; it provides a cost-effective security enhancement to Wi-Fi networks by Incorporating free but mature software tools; it can protect the network from adversaries capable of using customized equipment and violating the IEEE 802.11 standard**

***Keywords*: IEEE 802.11, RAP, Traffic Characteristics.**

1. Introduction

In computer networking, a wireless access point (WAP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a router (via a wired network), and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.

Wireless security concerns

It is the prevention of unauthorized access or damage to computers using wireless networks. Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

One of the most challenging security concerns for network administrators is the presence of rogue wireless access points. A rogue access point (RAP) is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network management or has been created to allow a cracker to conduct a man-in-the-middle attack.

The rogue access points are devices that are deployed in secure WLANs without permission or knowledge of the network administrator. The presence of such rogue access point poses severe threats to the WLAN security as it could compromise security of the entire wireless LAN. This problem has been in existence ever since WLANs have become popular in commercial applications. There have been reports of data theft, identity theft by using these rogue access points. Increasing use of wireless technologies by defence establishments along with above mentioned reasons have compelled researchers all over the world to find a solution for this problem. WLANs face the same security challenges as their wired counterparts, and more.

2. Literature Review

Common Approaches to Rogue AP Detection

The only way to reliably discover rogue APs is to listen to the airwaves – the wireless side of your network in combination with the wired side of your network. There are software and hardware products that make the former possible, In[1]An analytic model of prior probability distribution of Segmental TCP Jitter (STJ) is deduced from the mechanism of IEEE 802.11 MAC Distributed Coordinated Function (DCF) and used to differentiate the types of wire and WLAN connection which is the crucial step for RAPs detecting but on their own they offer incomplete solutions.

Sniffers

One way to find a rogue access point is to search your facility from the wireless side. Sniffer software (such as Air Snort or Nets tumbler) allows you to carry a laptop or PDA around your facility scanning all radio frequency (RF) channels for connections with any and all access points within range. While this software allows you to capture valuable information about the access points in your environment, it can be very time consuming to walk through all of your facilities in search of rogues. And data captured this way is only a sample snapshot – only valid when it is captured [2]. Further, you must determine whether the unrecognized access points you discover are rogue (within your facility whether connected to your network or not) or simply foreign (operating within range of your airspace, but connected to some other network, i.e. a neighboring business). While this type of RF audit is often worthwhile, it is costly, incomplete, and too intermittent to continuously protect your wired network from rogues. And if your network covers many geographically dispersed locations, this method of rogue detection may be unworkable.

Probes

To ensure continuous vigilance for rogue APs, you can install full-time probes – electronic devices that continuously monitor all Wi-Fi (802.11) traffic within their range. This can be an expensive proposition. Not just in the cost of the probes (typically $500 to $1000 per device), but also in terms of pulling Ethernet cable and providing electrical power.

According to a study by Gartner [3], rogue APs are present on about 20% of all enterprise networks The research community has just recently started to direct attention toward rogue AP detection. Architecture for fault diagnostics in IEEE 802.11 networks is presented in [4]. Multiple APs and mobile clients perform RF monitoring to help detect the presence of rogue wireless devices like unauthorized APs. Bahl et al. [5] propose a distributed monitoring infrastructure called DAIR. It attaches USB wireless adapters to desktop machines for more comprehensive traffic capturing ability Differences in inter-packet spacing between traffic flows on wired and wireless networks is used in [6] for identification of rogue APs. However, the scheme does not differentiate between wireless traffic from authorized and unauthorized APs. Multiple network sniffers are used in [7] for detecting rogue APs and eavesdroppers. Each sniffer has three network cards, and the intrusion detection capabilities are stymied byMAC address spoofing Yeo et al. [8] improve the performance of wireless monitoring by merging packet captures from multiple network sniffers and carefully selecting sniffer placement There are also easy-to-use and freely available tools such as FakeAP that allow an individual device to masquerade as multiple APs. Although intended to obfuscate a network's presence to war drivers, the software can also be used to confuse legitimate users of networks with similar SSIDs.

3. Proposed method and architectural view

It is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can ignorantly or maliciously install an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points. Presence of large number of wireless access points can be sensed in airspace of typical enterprise facility. These include managed access points in the secure network plus access points in the neighborhood. Wireless intrusion prevention system facilitates the job of auditing these access points on a continuous basis to find out if there are any rogue access points among them. Active node is any connected system in a wi-fi region which can transfer the packets to and from network within or outside of the network.

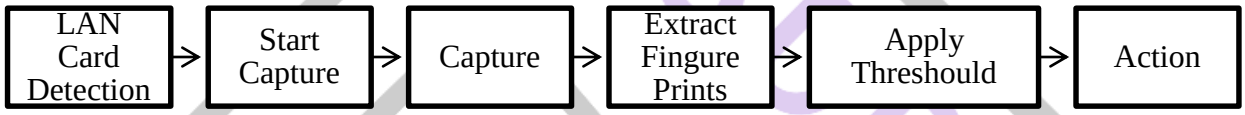

Figure 1.0 Data flow diagram

It is common practice to draw the context-level data flow diagram first, which shows the interaction between the system and external agents which act as data sources and data sinks. On the context diagram the system's interactions with the outside world are modelled purely in terms of data flows across the system boundary. The context diagram shows the entire system as a single process, and gives no clues as to its internal organization.

This context-level DFD is next "exploded", to produce a Level 0 DFD that shows some of the detail of the system being modeled. The Level 0 DFD shows how the system is divided into sub-systems (processes), each of which deals with one or more of the data flows to or from an external agent, and which together provide all of the functionality of the system as a whole. It also identifies internal data stores that must be present in order for the system to do its job, and shows the flow of data between the various parts of the system.

4. Proposed RAPD algorithm and results

This topic will enhance the results of system for proposed RAPD algorithm for given network scenario under consideration. The system will subject to capture the packets from access point in packet collector module. Then collected packets are sent to Preemption engine and Detection engine respectively. Further the packets are analyzed by Probing functions for checking access point is rogue or not.

Figure 2.0 Available Networks in Wireless Range

The Figure 2.0 shows four Access Points (APs) available in current scenario detected by the wireless LAN drivers of system. The Access Point names or also called SSID are D-Link-Dir-524-2, Comp, WIN-COEPVODDNST-60130 and Micromax A116 respectively are available in the current wireless network. The parameters which are under our area of interest for RAPD algorithm are MAC address, SSID, Security Type, Signal utilized and Channel number are stored in systems Database together in text file present inside system under consideration, which wants to connect the access point present in the entire network.
After performing the selection of wireless LAN driver (Microsoft) we can monitor the complete wireless traffic using all the packets transfer from source to destination, with their MAC addresses and IP addresses through all the access points in the current network After checking of traffic transfer from source to destination means network is visible to our LAN card by connecting any random-access point may be rogue or not. Now our RAPD algorithm will come into action before connecting to any access point, click the Scan button as shown in figure 4.3, the system will start checking available access points in the current network scenario by using traffic flow with packets having parameters like SSID, MAC Address, Signal etc. broadcast by all the access points over entire wireless network continuously.

MACAddress	SSID	Channel	Security	Signal
0:25:c2:d7:93:65	WIN-COEPVODDNST-60130	11	WPA2-Personal	802.11n
f0:1e:a6:08:27:18	Comp	11	Open	802.11n
f2:b3:3f:9d:cd:29	Micromax A116	1	Open	802.11n
f8:a3:86:8a:13:5a	D-Link_DIR-524	11	WPA-Personal	802.11n
f0:1e:a6:08:27:18	Comp	11	Open	802.11n

Figure 3.0 All Available Access Point with Information Gathered

Now, the environment with multiple number of access points is available, by simply clicking on Scan button as shown in figure 4.0 System can identify the rogue access points by executing the proposed RAPD algorithm iteratively for available access points in the current network with list of all rogue access point present for current scenario. As shown in figure 4.5 for all unauthorized packet transfer and total packet counter with MAC Address and SSID broadcast by the rogue access point through current network.

Fig. 4.0 Rouge Access Point List Detected in Network

5. Decision Making

The core part of algorithm is mentioned in the table 4.1, Where Detection Engine and Preemption Engine with all five parameters shows the working of the proposed RAPD algorithm with column Threshold will gives the access point's specification whether it is authorized or rogue access point to connect the system present in the environment for access the network.

Table 1 Possibilities for Detection Algorithm

MAC Address	SSID	Channel	Security	Signal	Type
DETECTION ENGINE		**PREEMPTION ENGINE**			**THRESHOLD**
Registered	Unregistered	Known	Known	Correct	Authorized
Unregistered	Registered	Known	Known	Correct	Authorized
Registered	**Registered**	**Unknown**	**Unknown**	**Incorrect**	**Authorized**
Unregistered	Registered	Unknown	Unknown	Incorrect	Unauthorized
Unregistered	Unregistered	Unknown	Unknown	Incorrect	Unauthorized
Unregistered	**Unregistered**	**Known**	**Known**	**Correct**	**Unauthorized**
Unregistered	Registered	Known	Known	Correct	Authorized
Registered	Unregistered	Known	Unknown	Incorrect	Unauthorized

6 Graphical Analysis of Rogue Access Point

The new algorithm is proposed by system called RAPD algorithm, which will detects the rogue access point existence in the available networks for a system to connect public network via access points available in current scenario. The algorithm is efficient and cost effective without making any change in existing system, only software is installed on the system/device wants to connect to wireless network. So system wants to connect to the network through access point can easily find rogue access point in the network without any special hardware.
Then analysis for rogue access point can be determine in graphical form as given below,

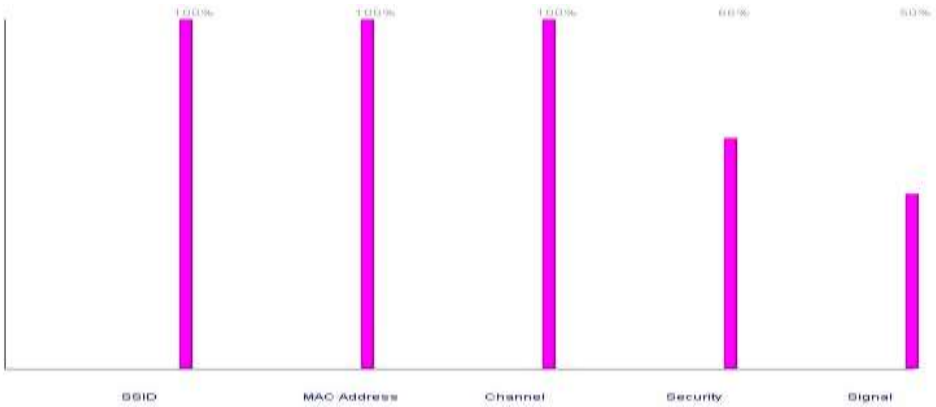

Fig. 5.0 SSID, MACID, Channel (100%) with Security (66%) and channel (50%)

As shown in figure 6.0 all SSID are registered in the system, only one channel that is channel no.1 is registered to the system and the open security is registered. By comparing the given graphical representation, the access point having SSID as comp is made authorized. Runtime we can make the parameters register by clicking Enter Data button as shown in figure 4.3, But we need to restart the system for changes to be takes place.

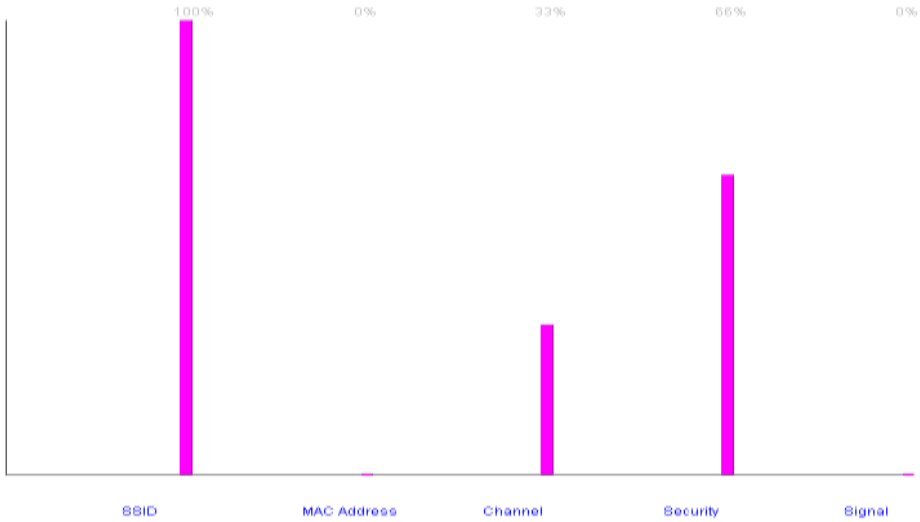

Fig. 6.0 All SSID, Channel (1) & Security (Open) Registered.

Hence form above discussion it is clear that we can find the unauthorized AP by using only 4 parameters in effective and faster fashion. And you also can take the help of other parameters required for make the faster decisions and more effective system. But it again ingress the system overheads and decrees the network performance.

6. Conclusion

We provided a comprehensive taxonomy of Rogue Access Points. Our classification of Rogue Access Points (APs) includes improperly configured APs, phishing APs, unauthorized APs, and a new class of rogue AP termed as compromised APs. The proposed technique is effective and low cost, designed to utilize the existing wireless LAN infrastructure efficiently and effectively. Also, no need to acquire the new radio frequency devices or dedicated wireless detection sensors separately for any current wireless network. The system uses the various available parameters coming from the packets over wireless network to detect the Rogue Access Point, without affecting the networks performance. The experimental results in the real system are demonstrated; the system can find Rogue Access Point existence in network without specified hardware or change in existing setup done by network admin as we having only plug and play software The proposed algorithm (RAPD) works efficient for the multiple numbers of access points present in current environment with multiple SSIDs and MAC Addresses available. As per graphical analysis it can be concluded that, the proposed algorithm required less time to execute with more efficiency in results after multiple iterations are completed over entire network for all available access points. The proposed algorithm is easily implemented and executed in less time with good performance for any wireless network that follows IEEE 802.11 security standards.

In future work, we can extend the proposed algorithm of Rogue Access Point detection for the more parameters of packets and evaluated by preemption engine and detection engine by selecting primary and secondary parameters respectively for a wireless network having higher chances of introducing Rogue Access Points or network which requires more security like military networks. We also can use different data mining techniques to detect Rogue Access Points in wireless network. The proposed system will only detect the Rogue Access Point available but user using the wireless device on network can connect to the access point manually,

so prevention also can be included after detection of Rogue Access Points. So, user must not connect to such access point and network is not under any attack.

REFERENCES

1. **Bandal Ganesh B., Dhamdhere Vidya S.,and Pardeshi Siddharth A.,** "*Rogue Access Point Detection System in Wireless LAN*", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2 Issue5, Oct-2012, PP6-11.
2. **Gaogang Xie, Tingting He, Guangxing Zhang**,"*Rogue Access Point Detection Using Segmental TCP Jitter*", WWW Poster Paper, Beijing, China ACM 978-1-60558-085, April-2008.
3. **Prof. Vanjale S. B.,** "*Distributed Rogue Access Point Detection in IEEE 802.11 Wireless Lan Using Mobile Agent*", International Conference on Advanced Computing Technologies (ICACT), April-2008.
4. **Technical Support Document,** *"Control and Provisioning of Wireless Access Point Protocol Rogue Management in a Unified Wireless Network*", Cisco Systems and Document ID112045, Aug-10, http://www.cisco.com/en/US/docs/wireless/controller /7.2/configuration/guide/cg_lwap.pdf.
5. **Technical Whitepaper,** "*Air Magnet: Best Practices for Rogue Detection and Annihilation*", Nov–2004, http://airmagnet.flukenetworks.com/assets/whitepaper/ Rogue_Detection_White_Paper.pdf.
6. **Beetle and Potter Bruce,** "*Rogue Squadron: Evil Twins, 802.11intel, Radical Radious and Wireless Weaponry for Windows*", Black Hat USA, Nov-2005, http://airsnarf.shmoo.com/rogue_squadron/twins.pdf.
7. **Beyah Raheem, Kangude Shantanu, George Yu and Strickland Brian,** "*Rogue Access Point Detection using Temporal Traffic Characteristics*", Nov-10, http://www.airwave.com/airwave_rogue_detection.pdf.
8. **An ISS Technical White Paper,** "*Wireless LAN Security*", 6303 Barfield Road Atlanta GA 30328, Dec-11, PP1-9, http://www.isaac.cs.berkeley.edu/ isaac/wep-faq.html.
9. **White Paper**, "*Rogue AP and Rogue Client Detection, Wlan Access Point*", June-10, PP1-10, http://www.e-catalog.beldensolutions.com/download/P_id-25.pdf.
10. **White Paper,** "*Solution for Detecting & Eliminating Rouge Wireless Network*", Oct-11, PP1-10, http://www.motorolasolutions.com/web/Business/Products/Software/~ /AirDefense Security_ Compliance/ documents/Static_files/Tired_of_Rogues.pdf.
11. **White Paper**, "*Solutions for Detecting and Eliminating Rogue Wireless Networks*", Air Defense, May-2008, PP 1-10, http://www.tekrati.com/research/ News.asp?id=5764.
12. **White Paper**, "*Wireless Network Rogue Access Point Detection & Blocking*", Manage Engine Advent net, Nov-2005, https://www.service-desk.co/white_papers/wifi_management_wp.pdf.
13. **Reference Manual,** "*16 AP Wireless Management System WMS5316*" Net Gear Pro Safe, 202-10601-02, Drive San Jose, CA 95134 US, July-10, https://*www.netgear.com/upload/product/wms5316/wms5316_ds_01apr10.pdf*.
14. **Data Sheet** "*16-AP Wireless Management System*", Pro Safe1-888-Netgear, July-10, http://www.netgear.com/prosafe_888.pdf.
15. **Karygiannis Tom, Owens Les,** "*Wireless Network Security 802.11, Bluetooth and Handheld Devices*", NIST Special Publication, Nov-12, http://csrc.nist.gov/publications/ *nistpubs/800-97/SP800-97.pdf*.
16. [**Purbo Onno and Buettrich Sebastian,** *"Access Point Configuration*", April-06, https:// *wirelessu.org/units/list*.
17. **Management and Configuration Guide,**"*Wireless Access Point 530*", Procurve 5991-2193, April 2006, http://www.procurve.com.
18. **Ahmad Amran and Hassan Suhaidi,** "*Detecting Rogue Access Point (RAP) using Simple Network Management Protocol (SNMP)*", International Conference on Network Applications, Protocols and Services, Nov-08, PP1-4.
19. **Guangzhi Qu, Nefcy Michael M.",** RAPID: *An Indirect Rogue Access Points Detection System*", IEEE-978-1-4244-9328-9, Oct-2010.
20. **Han Hao, Sheng Bo, Tan Chiu C., Li Qun and Lu Sanglu**, "*A Measurement Based Rogue AP Detection Scheme*", Infocom, Nov-2008, https://www.cs.wm.edu /~hhan/papers/info09_rogue.pdf
21. **Technical White Paper,** "Cloud Controller Product Manual for Wireless Systems", Meraki Production Product Manual St. San Francisco California, Dec-2011, https://www.meraki.com.