Analysis of security in wireless network: Architecture

[1]Abhimanyu Dnyandeo Sangale, [2]Dr.Sanjeev Kumar Sharma
[1]Research Scholar, [2]Research Guide, Oriental university, Indore (MP), India.
[1]abhimanyu.sangale@gmail.com, [2]spd50020@gmail.com

Abstract: **- The most challenging security concerns for IT industries today is the rogue wireless access point. Now a day's IEEE 802.11 technologies continue to become more popular, less expensive, and easier for end users to install, the threat to corporate network security are increases rapidly. Most of the current approaches to detecting rogue APs are easily evaded by hackers. In Our paper, we proposed a very new algorithm and architecture to detect the RAP in wireless networks, without change in existing hardware. We simply monitor the traffic and its characteristics in our system to detect the RAP (Rouge Access Point) and make the wireless network more secure for data transfer.**

This paper focuses on the RAPD Rogue Access Point Detection (RAPD) algorithm a method with flow chart and some proposed theory for future work to find the RAP and make the system more secure in wireless era which uses IEEE 802.11 standards for communication.

Keywords- IEEE 802.11, RAP, Traffic Characteristics.

I. INTRODUCTION

A rogue AP is an unauthorized access point plugged into a corporate network, posing a serious security threat to enterprise IT systems. Rogue APs are typically installed by employees in work places for convenience and flexibility. Although users could leverage common security measures such as Wired Equivalent Privacy (WEP) to protect their network communications, such measures may not be consistent with the corporate security policies and they are often inefficient. For example, researchers have identified design flaws in WEP, which can be easily exploited to recover secret keys

Rogue AP exposes internal networks to the outside world, making it easy for people to bypass security measures. A compromised AP is the most dangerous rogue AP that can exist in commodity Wi-Fi Networks. In particular, it is difficult to detect such a rogue device because the AP itself is not malfunctioning (e.g., operating without specified security controls)

outsiders. It is important to clarify where RAP fits into the larger hierarchy of insider threats [4].

In this paper, we summarize the rogue access point as two definitions: − Definition 1: Rogue access point is the access point that is installed to the network without authorization and does not follow the organization's security policy. − Definition 2: Rogue access point is the access point that is setup based on the malicious intention to compromise the company's information system i.e, data sniffing going through the rogue access point. An access point with the criteria that falls in either definition is considered to be the rogue access point. There are four common types of rogue access point as the follows:

1. Employee's rogue access point: Employees buy an access point and installs it on the company's LAN for their own convenient uses without the authorization. The rogue access point creates the vulnerability to the network. It enables unauthorized users or attackers from outside to access the company's network. This type of rogue access point is very common especially in the organization that is lacking of the wireless security policy and security awareness training for employees.

2. Attacker's external rogue access point: The rogue access point is setup outside the company and does not connect to the company's network. Typically, the attacker will use the high transmission power and high antenna gain rogue access point with the spoof SSID. It aims to allure the target employee to connect the rogue access point. All user traffic is redirected through the rogue access point and analyzed by the attacker.

II. LITERATURE REVIEW

Russell [1] discussed several methods of detecting RAP like SNMP scanning, TCP fingerprint, active probing and RF Monitoring. Watkins et.al. [2] propose to use the round-trip time (RTT) of network traffic to distinguish between wired and wireless nodes and the lower capacity and the higher variability in a wireless network can be used to effectively distinguish between wired and wireless nodes remains valid as the capacity of wired and wireless links increase, and is

 DOI : 10.35291/2454-9150.2022.0101

independent of the signal range of the rogue APs. Mohan and Byram [3] propose a distributed agent-based intrusion detection and response system for wireless LANs that can detect unauthorized wireless elements and system reacts to intrusions by either notifying the concerned personnel, or by blocking unauthorized users from accessing the network resources. Pro Curve networking [4] wills tell how to set a wireless network and what are the basics of IEEE 802.11 Standards which are required in setting WLAN.

Atul et.al. [7] Presents architecture for detecting and diagnosing faults in IEEE 802.11 infrastructure wireless networks, address fault diagnostic issues for these networks. Propose and evaluate a novel technique called Client Conduit, which enables bootstrapping and fault diagnosis of disconnected clients, built a prototype of our fault diagnostic architecture on the Windows operating system using off-the-shelf IEEE 802.11 cards. It imposes low overheads when clients are not experiencing problems. Paramvir Ranveer et.al.[8] present a framework for monitoring enterprise wireless networks using desktop infrastructure called DAIR, which is Dense Array of Inexpensive Radios, DAIR framework is useful for detecting rogue wireless devices (e.g., access points) attached to corporate networks, as well as for detecting Denial of Service attacks on Wi-Fi networks. Flute Networks [9] in white paper gives Solutions which are available to help a network manager detect the presence of a rogue AP on his network like most common search methods ``convergence" method and the "vector" method to locate the RAP in the network.

III. PROPOSED METHOD AND ARCHITECTURAL VIEW

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 from Normal Mode to Sniffer Mode and operates as wireless sniffer collecting wireless sniffing data including Beacon, Probe messages and client data frames.

2) Wireless sniffing data will be normalized to remove irrelevant information out and store the rest to the database. Detecting & Eliminating Rogue Access Point in IEEE 802.11 WLAN 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. The algorithms are the follows:

1) Compare the sniffing data (i.e., SSID, Wireless MAC, RF, etc) with the authorized AP information. The authorized AP information is stored beforehand. There are three possible outcomes: Completely Matched, Completely Unmatched, and Partially Matched parameters. If Completely Matched, Go to stage 2). If Partially Matched, go to stage 3) and If Completely Unmatched go to 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. 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 include the timestamp on the Beacon. The timestamp is the 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 the timestamp of the trusted AP.

3) For Partially Matched, the result would be either Mis-configuration AP or Attacker's Rogue AP. The mis-configuration 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 Mis-configuration AP and leave the remainder 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 an Employee rogue AP. The technique to perform "AP internal connection checking".

The proposed system works on basically four main modules 1. from the beacon frames the packets are separately sorted with various traffic characteristics parameters like SSID, MAC address, Signal, Security, channel used etc. And the probing function will take the decision depending upon the algorithm whether the given access point is Authorized or unauthorized. As shown in figure 1.

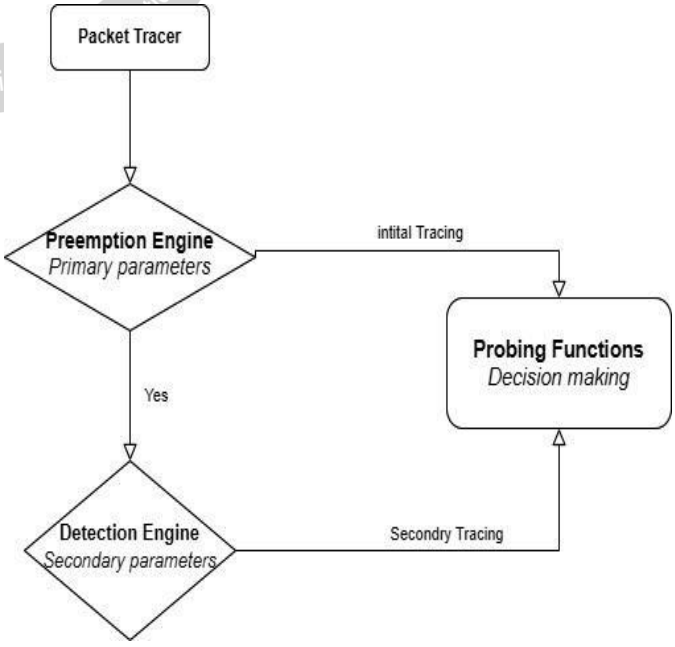

Figure 1: - Proposed Architecture

 DOI : 10.35291/2454-9150.2022.0101

IV. PROPOSED RAPD ALGORITHM AND FLOWCHART

1) Compare the SSID and MAC address of the selected AP with the AP available in the database. There are three possible outcomes: Completely Matched, Completely Unmatched and Partially Matched. Then depending on that take, the next step

A. completely matched; go to stage 2).

B. partially matched; go to stage 3)

C. Completely Unmatched go to stage 4)

1) For completely matched, then the AP we try to connect is: Trusted AP. So no need to go for Preemption Engine

3) For partially matched, then AP is incorrect configured AP or Attacker's RAP. If its attackers AP then it will check for the preemption engine.

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

2) For completely matched, there is maximum possibility of access points: Trusted AP. Then there is no need to check other traffic parameters from the incoming beacon frame & call that AP as authorized AP and the user can share its data with that AP.

3) For partially matched Information about AP, It initially assumes that its Attacker's RAP. And then the algorithm will terminate with the result as RAP is found don't connect to that AP.

Figure 2 shows the flow chart above proposed algorithm

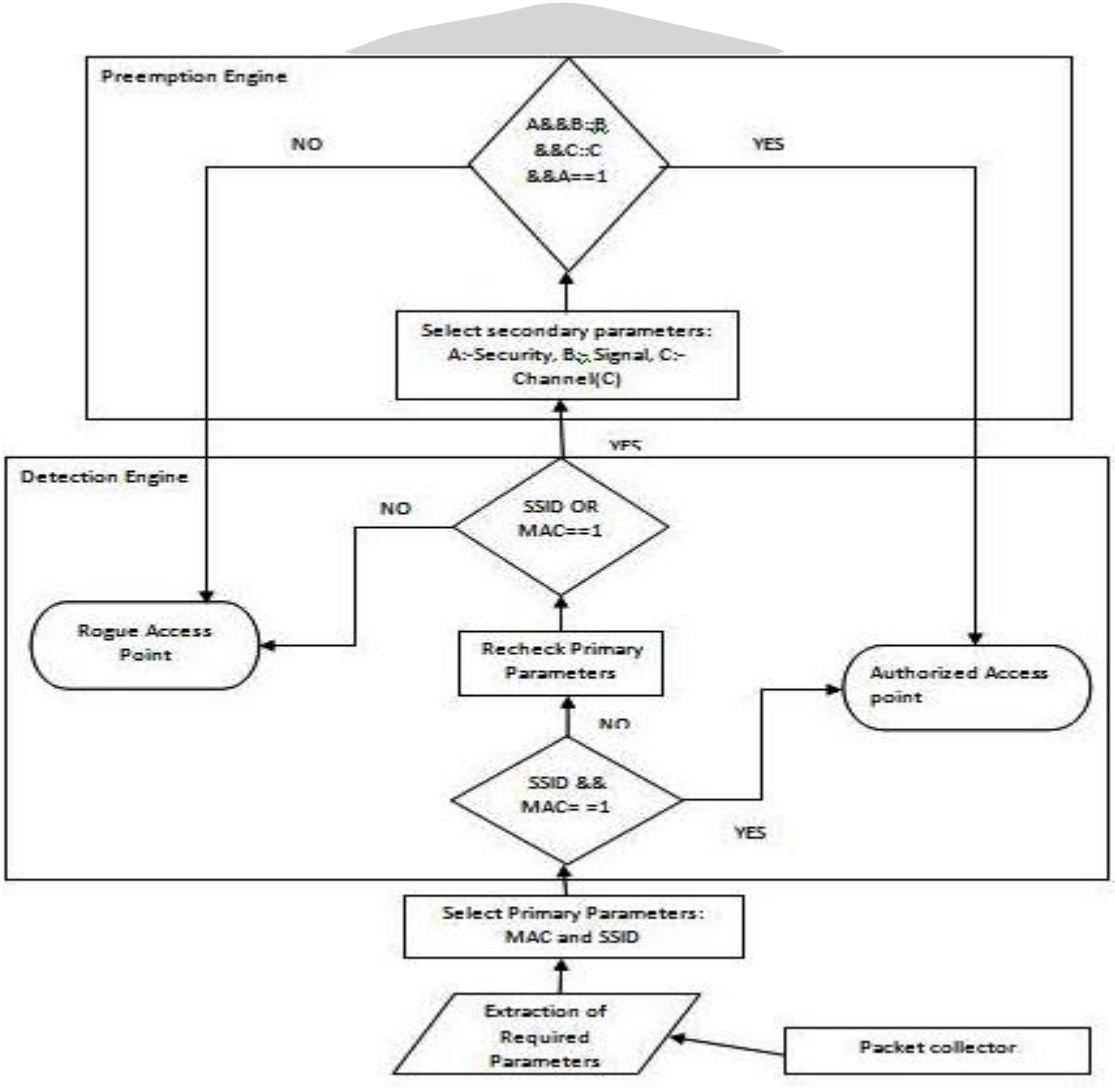

Figure 2.0: - flow chart for RAPD algorithm

 DOI : 10.35291/2454-9150.2022.0101

V. DECISION MAKING

The core part of algorithm is mentioned in the table 1.0, 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

As per network scenario under consideration RAPD algorithm applied on given set of access points, which shows access point having SSID comp is authorized while for access point with SSID Dlink_dir_524 as unauthorized as shown in figure 4.5. For all possibilities as mentioned in table 4.1 the proposed RAPD algorithm will work correctly and effectively for checking the parameters and matching parameters threshold values to decide whether it is rogue access point or authorized access point

Table 1.0 Possibilities for Detection Algorithm

Parameter	MAC Address	SSID	Channel	Security	Signal Type	TYPE
Phase/Sr. N0	**Detection Phase**		**Preemption Phase**			**Decision**
1	R	UR	K	K	Co	Authorized
2	UR	R	K	K	Co	Authorized
3	R	R	U	U	IC	Authorized
4	R	UR	K	UN	IC	Unauthorized
5	UR	UR	K	K	IC	Unauthorized

Notations: - UR: - Unregistered, R: - Registered, K: -Known, UN: -Unknown, Co: -Correct, IC: -Incorrect

VI. CONCLUSION

The proposed algorithm will be uses mainly for the wireless security, it detects the Rouge Access Point (RAP) present in the network by using various parameters associated with the wireless communication as the data loss in wireless communication is more so we should prevent the wireless system from such losses. RAPD stands for Rogue Access Point Detection. 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.

REFERENCES

[1] Russell Steve, "*Detecting and Locating Rogue Access Point*", April-2003, http://www.ee.iastate.edu/~russell/cpre537.s04/Report-Example.pdf.

[2] Lanier Watkins, Beyah Raheem, and Corbett Cherita, "*A Passive Approach to Rogue Access Point Detection*", GLOBECOM IEEE Proceedings 1930-529X, Sept-2007, PP355-360.

[3] Chirumamilla, Mohan K and Byrav Ramamurthy, "Agent Based Intrusion Detection and Response System for Wireless LANs" IEEE International Conference on Commun-ications, May-2003, PP492–496, http://digitalcommons.unl.edu/cseconfwork /64.

[4] Technical White Paper, "A Wireless Networks", HP Procurve Networking's, June-2006, http://www.procurve.com.

[5] Hongda Yin, Guanling Chen, and Jie Wang, "Detecting Protected Layer-3 Rogue APs" Broad net, Oct-2007, http://www.cs.wm.edu/papers/info09_rogue.pdf.

[7] Adya Atul, Bahl Paramvir, and Chandra Ranveer, "Architecture and Techniques for Diagnosing Faults in IEEE 802.11 Infrastructure Networks", MobiCom'04, Philadelphia Pennsylvania USA, ACM 1-58113-868-7, Sept-2009.

[8] Bahly Paramvir, Chandra Ranveer, Padhyey Jitendra, Ravindranathy Lenin Manpreet, Singh, Wolman Alec, and Zilly Brian, "Enhancing the Security of Corporate Wi-Fi Networks Using DAIR", MobiSys'06, Uppsala, Sweden, ACM 1-59593-195-3, June-2006.

[9] White Paper, "Locating Rogue Wireless Access Points", Fluke Networks, https://www.flukenetworks.com.

[10]Airdefense White Paper: 'Wireless LANs: Risks and Defenses', Available Online: http://www.itsec.gov.cn/webportal/download/73.pdf

[11] Raheem Beyah and Aravind Venkataraman," Rogue Access Point Detection:Challenges, Solutions and Future Directions", This article has been accepted for publication in IEEE Security and Privacy.

[12] A. Adya, P. Bahl, R. Chandra, and L. Qiu. Architecture and techniques for diagnosing faults in ieee 802.11 infrastructure networks. In

MobiCom '04, pages 30–44. ACM Press, 2004

[13] Liran Ma, Amin Y. Teymorian, Xiuzhen Cheng," RAP: Protecting Commodity Wi-Fi Networks from Rogue Access Points".

[14] Airdefense White Paper: 'Solutions for Detecting and Eliminating Rogue Wireless Networks', Available Online: http://www.airdefense.net/whitepapers/index.php

[15] Ma, L., Teymorian, A.Y., Cheng, X.: 'A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks', IEEE INFOCOM, 2008.

 DOI : 10.35291/2454-9150.2022.0101