IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

Unauthorized Access Point Detection Methods in 802.11 : A Review

Mr. Mitesh G. Patel[1] and Prof. (Dr.) Nilesh K. Modi[2]
Campus Director, Asian Institute of Technology, Vadali[1]
Professor & Director, School of Computer Science, BAOU, Ahmedabad[2]
mca.mitesh@gmail.com[1] and nilesh.modi@baou.edu.in[2]

Abstract: *Unauthorized access point are unwanted whether they are access points or rogue access point or clients. They steal our critical information and not only steal our data but also execute malicious application into our network. "Free Wi-Fi" now a day's this word become more popular due to free of cost. Public places like bus station, restaurant, malls etc. having a device like wireless access point through which they provide service to the end user. To detect a unauthorized access point different approaches are used. These approaches are briefly classified as client-side approach, Server-side and Hybrid approach. Every approach has its own pros and cons. As we know clients have limited resources and do not possess much control over network when compared with servers. Amongst all available approaches Hybrid approach is efficient because it minimizes the inabilities of client side approach and adds server control for detection of Unauthorized AP. The motive of this paper is to surveying different methods of unauthorized access point detection.*

Keywords: Rogue Access Point, Server-side Approach, Hybrid approach, IEEE 802.11, Unauthorized AP, Client-side Approach.

I. INTRODUCTION

As we all know very well IEEE 802.11 standards are popularly known as Wireless Local Area Network (WLAN), Wireless Ethernet, Wi-fi, Hot-spot. Currently, wireless network communication, such as 3G, 4G, 5G serves as a basic infrastructure for internet access. Wi-fi is the most preferable choice owing to its high data rate, low or no service charges, and high availability. IEEE 802.11 enables cheap deployment and can be used to cover areas where cables cannot be used so that's why it is widely used in corporate offices as well as college campuses and for home also. Security has always been a concern in communication networks as it is in many other areas. The important typical security issues that one should consider are, threats to the physical network, unauthorized access to network resources, internal and external attacks. In the context of wired LAN's the solutions to the above issues are well defined and are fairly reliable. The same approaches, however, cannot be directly adapted to IEEE 802.11.

1.1 Rogue Access Point

An access point is a station which receives and transmits the data which is also known as transceiver. There are two types of access point can be set up with mostly different equipment's. The first type uses a wireless router connected directly into an Ethernet jack on wall. The another second type are set up on a portable laptop with two wireless cards one connected to a real AP and the other configured as an AP to provide internet access to WLAN Station Due to the various smart devices the existence of Unauthorized AP has become unavoidable.

1.2 Intrusion into IEEE 802.11

Intrusion, in wireless network, is described as the act of wrongfully accessing the network resources without having appropriate privileges. Intrusion into wireless networks is relatively easier when compared to wired networks. Wireless networks are highly susceptible to intrusion because of the radio technology that is being used. Wireless has opened a new and exciting world for many of us. Its technology is advancing and changing every day and its popularity is

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

increasing. The biggest concern with wireless, has been security. The traditional wired IDS (intrusion Detection System) is great system, but unfortunately it does little for the wireless world.

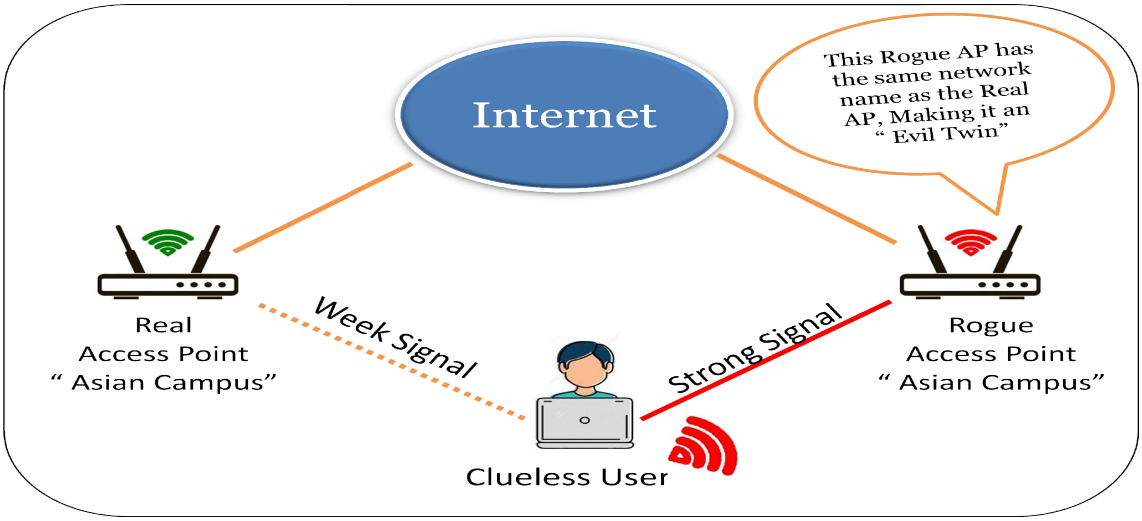

Figure 1: Unauthorized/Rogue Access Point Scenario.

II. Our Contribution

The Main Contribution of this paper is that it classifies different Unauthorized access point detection methods according to their implementation and suggests that which approaches or methods are efficient. In this paper, Unauthorized APs have been classified many times as wired and wireless according to set up. Unauthorized access point can be directly connected to Ethernet Jack (RJ45) using cables or can be set up using a laptop having two wireless network interface cards, for that Linux commands can be also used to bridge packets from one wireless network interface to another wireless network interface card. In Table I classification of Unauthorized access point detection methods on the basis of wired and wireless access point is given. The remaining part of the paper is organized as follow. In section II we have briefly discussed different approaches to detect Unauthorized access point. Here we preset a short discussion on each approach and describe in short different rogue AP detection methods along with their pros and cons. And at last section III concludes the paper.

III. Access Point Detection Methods

3.1 Round Trip Time

This is a client side Access Point detection methods which is also known as Round Trip Delay methods. Round Trip Time (RTT) is the length time it takes for a data packet to be sent to a destination plus the time it takes for an acknowledgment of that packet to be received back at the origin. The RTT between a network and server can be determined by using the ping command. This time delay also includes propagation times for the paths between the two communication points. According to 802.11 mechanism the delay for transmitting a packet can be calculated as : Delay for transmitting a packet = time for retransmission if no ACK is received + data transmission time + random back-off time + time deferred due to a busy channel medium + certain period of time for which channel is free.

Round Trip Time method required for DNS and probe which will give a time which is used for detecting Unauthorized AP as a threshold. According to experiment it required 1.3 ms. for Rogue AP time difference between RTT for probe and RTT for DNS server is calculated which greater than 1.3 ms most of the time according to authors' experimentation. As, there is a Rogue AP in between station and legitimate access point there will be one extra hop and will increase the time delay as shown in fig.3. The disadvantage of this method is that it can't identify Rogue APs connected to the wired network.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

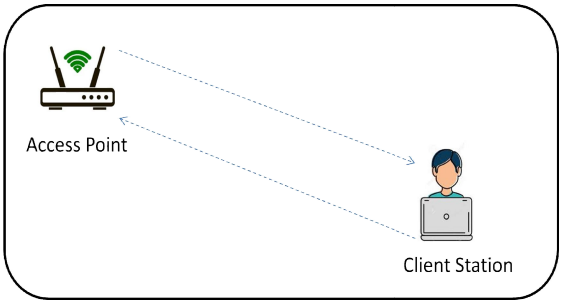

Figure 2: RTT Scenario When AP is Legitimate.

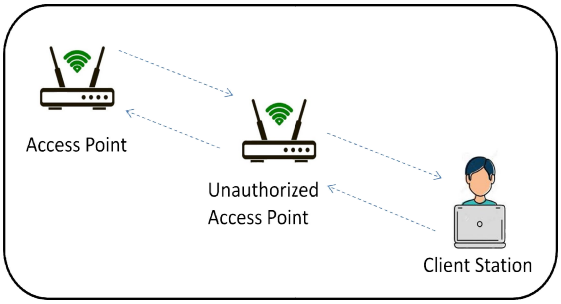

Figure 3: RTT Scenario When Unauthorized AP is Established. One Extra Hop.

3.2 Received Signal Strength & Seq. Hypothesis

This is a client side Access Point detection methods which is also known as Signal Peptide. This method is usually invisible to a user of a receiving device because signal strength can vary greatly and affect his functionality in wireless networking. RSSI can be used internally in a wireless networking card to determine when the amount of radio energy in the channel is below a certain threshold at which point the network card is clear to send (CTS). Once the card is clear to send, a packet of information can be sent. The end-user will likely observe a RSSI value when measuring the signal strength of a wireless network through the use of a wireless network monitoring tool like Wire-shark, Kismet or In-slider.

3.3 Clock Skew

This is a Server Side Access Point detection methods which is also known as Timing Skew. Clock Skew is a physical characteristic used by a access point. The instantaneous difference between the readings of any two clocks is called their skew. The operation of most digital circuits is synchronized by a periodic signal known as a “Clock” that dictates the sequence and pacing of the devices on the circuit. Clock skew have limitation due to differences in physical composition, temperature, and path length.

3.4 Hybrid Framework

This is a Server Side Access Point detection methods. The hybrid framework works with security protocols such as WEP and WPA. It does not require any specialized wireless hardware. The advantage of this method is it’s a cost effectiveness.

3.5 Convert Channel

This is a Hybrid Access Point detection method. This method creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. Convert channels are exceedingly hard to install in real systems, and can often be detected by monitoring system performance. It suffer from low signal-to-noise ratio and low data rates.

3.6 Multi-Agent Sourcing

This is Hybrid Access Point detection method. Master agent generates slave agents according to the number of active unauthorized access point at that moment of time. The Slave agents are then sent away to the connected APs and they are cloned at APs. Whenever the cloned salve agent at the client system detects any new Access Point, it automatically builds and sends a information packet INFO containing SSID (Service Set Identifier), MAC Address (Media Access Control), Vendors Name, Channel Used of the Unauthorized AP to Clone Agent to the connected AP. The Slave Agent at the AP sends this information to its Master Agent on the Server. Then 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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

Access Point Detection Method Comparison						
Approach	Client Side		Server Side		Hybrid	
Methods	Round Trip Time	Received Signal Strength & Seq. Hyphothesis	Clock Skew	Hybrid Framework	Conert Channel	Multi-Agent Sourcing
Parameters						
RAP Detection Type	Wireless	Wired	Wired	Wired And Wiredless	Wired And Wiredless	Wired And Wiredless
Characteristics	No Assistance From 802.11 Operator	No Assistance From 802.11 Operator	-	Cost-Effective Used Open Source Software for Implementation	Uses Steganography	Independent of Wireless Technology
Synonyms	Round Trip Delay	Signal Peptide	Timing Skew			Self - Organized System
Short Name	RTT					MAS

Figure 4: Access Point Detection Method Comparison.

IV. Conclusion

As we seen that client side approach is constrained as compared to server side approach. Once we found that server security mechanism is week and turn out to be unsuccessful then client cannot refrain itself from connecting to unauthorized access point. If Client-side and Server-side detection method approaches are combined one efficient solution can be drawn which can be called as Hybrid approach in which clients and servers or unauthorized access points are actively involved. So, even if server security mechanism fails to secure the network, client will not be connected to unauthorized access point or rogue access point and thus will be safe. The ultimate goal is to safeguard the client's critical data and to avoid various attacks like Man-in-the middle, Denial of service etc. Under Hybrid approach there are two methods Covert channel and Multi-agent sourcing in which both clients and servers are actively involved and provide efficient solution. Covert channel method is an authentication mechanism and can be used to prevent and detect Rogue AP. This mechanism does not consider wired side. Apart, from these methods even Hybrid framework also provide good solution to detect and prevent Rogue AP as it covers wired and wireless side of the network.

References

[1]. Rouge Access point: A Threat to Wireless Society Prof. Abhijit S. Bodhe1, Dr.A.S.Umesh2 Iaetsd Journal For Advanced Research In Applied Sciences Volume 4, Issue 7, Dec/2017 ISSN No: 2394-8442.

[2]. Rogue access point detection methods: A review Article· February 2015 DOI: 10.1109/ICICES.2014.7034106, https://www.researchgate.net/publication/282924894.

[3]. S. Anmulwar, S. Srivastava, S.P. Mahajan, A.K. Gupta, V. Kumar, "Rogue access point detection methods: A review", Proc. ICICES '14, pp. 1-6, 2014.

[4]. "WLAN Security Today: Wireless more Secure than Wired," Technical Whitepaper by Siemens Enterprise Communications, July- 2008. Available at: http://www.rapid.co.uk/uploads/media/17/8353.pdf

[5]. Bodhe, Abhijit, S. R. Deshmukh, and S. P. Patil. "Wireless Networks-A RAPD Algorithm."

[6]. https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks).

[7]. https://en.wikipedia.org/wiki/Rogue_access_point.