Wireless LAN rogue access point

*Nattala Annie Supriya, MSc CyberSecurity, Northumbria University, London, United Kingdom*

**Abstract:** A wireless LAN rogue access point (RAP) is an unauthorized access point in a wireless network that has been maliciously added by a threat actor in order to harm the network, exploit money, or misuse the information stolen. This paper will look at how rogue wireless LAN access points can lead to local area network vulnerabilities. There are various types of rogue access points, as well as their impact on the network. Various detection methods from other academic sources are analyzed, and their advantages are discussed. Also, the technical background of the vulnerability and the best practices and systems that can mitigate the risks and prevent rogue access points from causing operational, monetary, or organizational damage

**Keywords**—Wireless LAN Rogue Access Points, 802.11, SSID, Evil twin, Detection Techniques and Wireless Network Security.

# Introduction

A wireless rogue access point that gained unauthorized access to a secure system without any legal permission or authorization from a local system administrator is known as a wireless LAN rogue access point. This can be the result of either a deliberate attacker or a well-intentioned employee. The rogue access point, which is employed in several assaults, including DoS (Denial of Service) and data leaks, is among the most prevalent wireless security risks. It is challenging to find genuine gadgets from fake ones. Nevertheless, any unwanted wireless devices functioning near the internal network must be considered rogue wireless devices that could be opening unauthorized access points, regardless of the intended use.

A rogue access point (RAP) can monitor your data during passive interception but cannot alternate the data. If you connect to a network with a malicious access point and enter your password on a website using HTTP, the malicious access point can read it. Then they can access the phone or laptop to snoop into the network and read some files that will compromise the confidentiality of your data. Also, another method may be used to gather a person's online trace. By analyzing DNS requests and other Internet data, the malicious access point may keep tabs on your online activities along with installing spyware or keyloggers and backdoors to the system. Personal details about oneself, such as the types of sites you frequent, may be made public via this profile. During active interception, a rogue access point can possibly interfere with your data. They have access to user data, may make any necessary changes to it, and then transport the modified user data to the desired endpoint.

Unfortunately, several more rogue access points, known as soft access points, are installed by employees with malicious intent or without proper training to gain access to the network. Such unauthorized access might be permitted by the IT Department's rules and the organization's policies. The network is being freely accessed by other hackers who work for nearby businesses. These access points are often low-cost and consumer-grade, and they are frequently only detectable over the air and never advertise their unauthorized existence in the network. Authentication and encryption are not enabled, often deployed in their default state in the network, posing a security risk. The ideal target for wardriving (The practice of using a laptop or smartphone to look for Wi-Fi wireless networks while traveling) is an unrestricted access point connected to the corporate network because building barriers may allow wireless LAN signals to get through. Each user that establishes a connection with a malicious access point must be categorized as a rogue user since it is going against the established, approved security controls and best practices recommended by the IT Department and the organization’s policies.

# Literature review

[5] Rogue access points (RAPs) are introduced by insiders more frequently than typical assaults, which start from outside the network. This minor infraction can have serious repercussions since it creates a secret backdoor for access to the network and entirely nullifies the substantial effort in network security. There are several methods for RAP detection, but none are 100% accurate. This issue requires awareness from businesses, governments, and academia and support for innovative detection techniques. [1] Considering everyone with accessibility to the facilities might carelessly or deliberately install any cheap Wi-Fi network that could allow unauthorized individuals to use any secure system, RAPs have been proven to be a security risk to big organizations with numerous employees. Employees can install RAPs and create extensive wireless networks in both industrial and military enterprises without the knowledge or consent of network management. The privacy of the entire network is seriously compromised by these RAPs. Company employees with bad intentions install RAPs to the network port hidden behind the company security system. The most fundamental security parameters on the RAPs are seldom enabled by employees, making it simple for the threat actors to gain unauthorized access to the network via the rogue access point and conduct a man-in-the-middle attack by listening in on internet activity.

The vulnerability scanners employ a probabilistic method that solely depends on recorded packet size to operate on the encrypted AP communication. To solve this issue, [4] Yin (2007) outlines a novel rogue AP detection technique. The method sends experimental data to the wireless edge using a validator on the internal wired network and then utilizes wireless port scanning to find rogue APs that are relaying the test messages. These restrictions apply to this [1] study's findings that wireless access points must be immediately connected to or only a single hop distant from the monitoring site. Secondly, while uploading data by wireless hosts, detection techniques are effective. Third, because the method relies on visual examination, it is challenging to identify RAPs automatically. In their innovative approach to rogue access point identification, Jana and Kasera [6] suggested identification of a rogue access point in a wireless local area network (WLAN), using the clock skew of each access point as a fingerprint. At that time, the main issue was the inability to recognize MAC (Medium Access Control) address spoofing.

Sequential hypothesis testing is used in two online methods that Wei et al. [7] presented for the identification of rogue access points. These algorithms keep monitoring incoming traffic at an aggregation point for suspicious activity, such as a router or gateway. Then it quickly decides what to do with passively gathered TCP ACK pairs. Without utilizing any hardware, Kao et alnovel's access point identification approach is shown in [8]. According to client-side bottleneck bandwidth, this approach determines how data packets with an IP address get routed from access points. The system administrators just monitor the packets passing through all the switch ports because the detection technique is an addition to the present access point selection policy. A statistically based strategy for rogue access point identification was put out by Shivaraj et al. [9] This method applies a Hidden Markov Model to quantify passive incoming packet collection at a gateway. Utilizing differences in packet inter-arrival time is the basic principle behind this method.

[14] The PrAP-Hunter has two wireless interfaces to generate traffic to a receiver (a server listening TCP connection) during detection. Channels 1 through 11 are sequentially and intermittently interfered with by the first interface (interference equipment). The target AP (Ch 11), to which the PrAP-Hunter connects, serves as a communication route between the PrAP-Hunter and the real AP (Ch 1). (Ch 11). The first to question whether the AP is relaying signals or not is PrAP-Hunter. When the PrAP-Hunter generates traffic for the receiver, data is sent on channels 1 and 11.As per PrAP-Hunter, if the interference device blocks data transmission on channel 11 as a result of interfering with channel 1, this is a credible indication that the target AP is wirelessly exchanging data. In this scenario, the associated AP must be a PrAP. This process is shown in the image below (Figure 1) with a legitimate access point and a malicious access point.

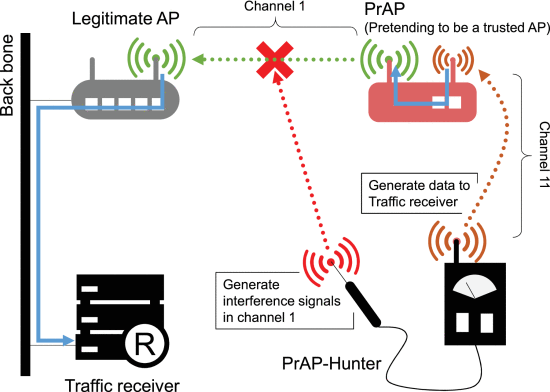


Figure 1: PrAP –Hunter Detection method

# TECHNICAL BACKGROUND OF ROGUE ACCESS POINTS

Rogue access points, denial of service (DoS), illegal client access, man-in-the-middle attacks, IP spoofing, hijacking, AP MAC spoofing, honeypot APs, and a host of other issues are just a few of the various difficulties that IEEE 802.11 encounters. [3] One of the most hazardous assaults is a rogue access point since it is an unauthorized AP that has been maliciously connected to the network by employees or guests of the company. Rogue access points (APs) are those that have been installed without the wireless local area network operator's consent [7]. Attacks stated above are made simpler to launch after the rogue AP is formed. It is an insider attack more so than an outside strike [5].

Controllers categorize unknown access points as members, neighbors, suspects, or rogues using a set of criteria, as shown in Figure 2.



Figure 2: How Scanned Information is Used to Classify Access Points

Dangers: Even though installing a soft access point or less-secure wireless router is technically simple for a well-intentioned employee, it is possible that they might configure this as "open" or with insufficient security, potentially granting access to unauthorized people, in order to make access from mobile devices easier. If an intruder sets up an access point, a threat arises that they run different system vulnerability scans and attack remotely instead from within the organization—as from the reception area, a nearby building, a parking lot, or even from several yards away with just a high-gain antenna. In the atmosphere of a typical company's site, someone might observe the existence of several wireless access points. These consist of both neighborhood access points and controlled access points in the secure network. The task of continuously inspecting these access points to identify any malicious access points is made easier by a wireless intrusion prevention system.

Two conditions must be verified to detect rogue access points:

i) In case an access point is in the managed whitelist of the access points list.

ii) Connection to the secure network

Comparing wireless MAC (Medium Access Control) addresses, also known as the BSSID, of the access point with the managed whitelist access point BSSID list makes it simple to test the first of the two requirements mentioned above. However, given the following circumstances, automated testing of the second criterion may be difficult: To assess access point connections in large-scale networks with just an adequate reaction time, examining a range of access point devices is important, including soft access points, NAT (router), bridging, and unencrypted and encrypted wireless communications. Additionally, it's important to avoid false positives and negatives, which are covered in more detail below. False positive happens in case an access point is not legitimately connected to the secure network and is mistakenly identified as a wired rogue by the wireless intrusion prevention system. Administrative resources are wasted pursuing false positives that occur often. In addition, the potential for false positives makes it difficult to enable the automatic blocking of wired rogues out of concern about blocking neighboring access points. False negatives happen when a wireless intrusion prevention system does not recognize a secure network-connected access point as a wired rogue. Security flaws come from false negatives. The first type of rogue access point is called a wired RAP and is present if a malicious access point is discovered to be physically connected to a secure network. In contrast, if the rogue access point is discovered and deemed to be external and unconnected to the secure network. If one of the external access points is discovered to be malicious or to pose a risk (for example, if its settings have the potential to attract or have attracted secure network wireless clients), it is labeled as a second type of rogue access point, sometimes known as an "evil twin."

There are many types of Rogue access points discussed below and their impact on the organization's network.

Neighbor Access Points: Typically; strong signals, ESSID, and frame rates are analyzed to determine how rapidly end devices join themselves to the access points. As a result, it's possible that authorized clients will mistakenly link to a neighboring AP that is not really connected to the company network. Although close APs (Access Points) may not be immediately threatening, nevertheless they will eventually leak information of the organization.

Ad Hoc Associations: Peer-to-peer Wi-Fi networks allow computers within the same network to share information with one another. This makes it easier to transmit files to others or send documents to a printer connected to Wi-Fi. It is often more difficult to detect or track this type of data crime because peer-to-peer communication skips network-imposed security measures like intrusion detection and encryption. Rogue access points in this network would cause damage immediately due to the lack of security measures.

Unauthorized Access Points: First, the most basic types of access points are easily available on the market. In an Evil Twin attack (MAC address), an A rogue actor creates rogue access points (AP) that precisely mimic the SSID and BSSID of a legal access point. The rogue access point will either emit stronger signals than the official AP or disable the real AP and substitute this to get people to sign up for it. That patient's and doctor's data has become accessible to the attacker because they unknowingly connected to the malicious AP. This opens the door for further harmful behavior. To intercept the session and get access to sensitive data, an attacker can engage in eavesdropping, traffic modification, and man-in-the-middle (MiTM) assaults. Attacks using evil twins may potentially give the offender total command over the entire network. According to the information collected and the tremendous demand for healthcare data on the dark web, healthcare companies make for incredibly alluring targets. It offers the seller substantial financial benefits. Threat actors would be keen to conduct an Evil Twin attack on institutions and hospitals that provide healthcare. Additionally, because of the industry's growing reliance on technology, bad actors have access to a lot of sensitive data. The likelihood of a cyberattack is further increased by several industry-specific risks.

# Recommendations and Suggestions to remediate the risks

There are a few actions and systems that the organizations can adapt to remediate this problem.

1. Establish regulations and policies explicitly for this purpose: Networks devices should be connected by authorized IT personnel. Every network-connected hardware, including wireless access points, complies with the corporate security guidelines.
2. Adapt the guidelines for identifying rogues: Unauthorized computers are automatically labeled as suspicious. When you set this to rogue, the controller automatically labels every customer or access point from a different network as rogue. You may then choose to isolate the offending access point by discarding any traffic from and through it.
3. Eliminating unnecessary APs so that malicious APs are evident: These access points cannot be categorized as rogues until secure connections' SSIDs and/or provider names are included in the list of SSIDs authorized on the system.
4. Blacklist known RAPs: Once a rogue access point is added to the rogue blacklist, it is blocked. The communications to and from access points are discarded.
5. IEEE 802.11 Security: The IEEE 802.11i security standard makes use of IEEE 802.1X for customers as well as networking verification. That implies that the system requires authorized customers before they may access system resources. Similarly, when initiating information transmission, the client confirms the legitimacy of the network infrastructure it is attached to. With 802.1X, authentication credentials like password protection are never transferred across the wireless channel unencrypted. Furthermore, dynamic per-user, per-session encryption keys are provided by 802.1X, which eliminates the complexity and security issues associated with static encryption keys. Security settings for WLAN profiles can be changed.
6. Scanning with active and passive access points: To find malicious access points and customers, operational scans transmit probes with a null SSID name. On radio profiles, the active scan is activated by default. It is advised against changing that parameter.
7. Monitor logs for suspicious activity: A supervisor automatically creates a recorded item if a rogue is found or leaves. Observe collecting Logs for Troubleshooting for more information.
8. Investigate Ad-hoc access points: The establishment of an ad hoc system is the outcome of direct communication between two client devices. The ad hoc networks expose the company to danger as they bypass the network's security procedures. Whenever an employee brings a laptop to the organization with wireless capabilities, plugs it into a wired connection, and leaves the wireless interface on, one of these threats arises. In this case, there would be a security risk because a hacker in the nearby vicinity may connect directly to the client. By simultaneously using the wired and wireless connections, the hacker may now search the employee's personal computer seeking information and breach the company's network. The organization might well be breaking regulations in its sector because of this predicament. The connection that ad-hoc access points offer into some other systems, rather than the ad-hoc network itself, is what creates the security vulnerability.
9. DHCP Server to assign Static IP addresses: While static IPs are assigned, a hacker that installs a malicious access point must manually assign the device an IP address to be able to join the network.
10. Port-based security is enabled on managed switches: If an access point is arbitrarily introduced into one of this switch's ports, it is unlikely to work.
11. Employ IDS/IPS: Systems like IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) aid in securing the network from malicious rogue access points. Wireless intrusion prevention solutions could be used to find unauthorized access points connected to your network. These devices can do thorough range scanning to identify all current internet connections.

# Conclusion and Further Studies

In any case, any organization must establish a proactive security protocol that specifies when Wi-Fi equipment is to be used, outlines the privacy risks related to it, and details the strategic plan and approval procedure required to adopt them in the environment. The potential repercussions for violating the policy should be mentioned. Furthermore, it should be noted that if automatic blocking is configured in the system, unauthorized access points will be blocked instantly. Finally, it is critical to set up a system for identifying fake access points, keeping an eye on real access points, and keeping track of peer-to-peer wireless connections. The best alternatives for addressing this are commercial solutions like AirDefense, AirMagnet, IBM Distributed Wireless Security Auditor or CA Wireless Site Management. Although these solutions are pricey, many have been designed particularly to meet this demand and include advanced capabilities that would be far more costly to build in-house. To determine whether the cost justifies the risk, cost-benefit analysis and risk analysis should be performed as usual. If the risk of an unreliable, exposed access point linked to the internal network is balanced in this analysis, then any firm with data that needs to be protected must have a robust rogue access point detection system.

*References*

1. S. Shetty, M. Song and L. Ma, "Rogue Access Point Detection by Analyzing Network Traffic Characteristics," MILCOM 2007 - IEEE Military Communications Conference, 2007, pp. 1-7, Doi: 10.1109/MILCOM.2007.4455018.
2. L. Watkins, R. Beyah, and C. Corbett, "A passive approach to rogue access point detection," IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference, 2007, pp.355-360, doi:10.1109/GLOCOM.2007.73.
3. L. Qawasmeh and F. Awad, "Tracking a Mobile Rogue Access Point," 2021 International Conference on Information Technology (ICIT), 2021, pp. 522–526, Doi: 10.1109/ICIT52682.2021.9491684.
4. Hongda Yin, Guanling Chen, and Jie Wang, "Detecting protected layer-3 rogue APs," 2007 Fourth International Conference on Broadband Communications, Networks, and Systems (BROADNETS '07), 2007, pp. 449–458, Doi: 10.1109/BROADNETS.2007.4550468.
5. R. Beyah and A. Venkataraman, "Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions," in IEEE Security & Privacy, vol. 9, no. 5, pp. 56–61, Sept.–Oct. 2011, Doi: 10.1109/MSP.2011.75.
6. Jana S. and Kasera S. K. (2008) On fast and accurate detection of unauthorized wireless access points using clock skews MobiCom 08, September 14-19, San Francisco, California, USA
7. Wei, W., Suh, K., Wang, B., Gu, Y., Kurose, J., and Towsley, D. (2007). Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs. Proceedings of the 7th ACM SIGCOMM Internet measurement conference (IMC '07).
8. Kao, K., Liao, I., and Li, Y. (2009), "Detecting rogue access points using client-side bottleneck bandwidth analysis," Science Direct, Computers & Security. 28- 144 –152
9. Shivaraj, G.; Song, M.; and Shetty, S. (2008). A hidden Markov model-based approach to detect rogue access points IEEE, 978-1-4244-2677
10. S. Nikbakhsh, A. B. A. Manaf, M. Zamani, and M. Janbeglou, "A Novel Approach for Rogue Access Point Detection on the Client-Side," 2012 26th International Conference on Advanced Information Networking and Applications Workshops, 2012, pp. 684-687, doi: 10.1109/WAINA.2012.108.
11. "WLAN Security Today: Wireless is More Secure than Wired", Technical Whitepaper by Siemens Enterprise Communications, July 2008.
12. Raheem Beyah et al., "Rogue Access Point Detection Using Temporal Traffic Characteristics," IEEE Communications Society, pp. 2271-2275, 2004.
13. Raheem Beyah and Aravind Venkataraman, "Insider Attack Rogue-Access-Point Detection Challenges, Solutions, and Future Directions," IEEE Security & Privacy, co-published by the IEEE Computer and Reliability Societies, pp. 56–61, September/October 2011.
14. R. Jang, J. Kang, A. Mohaisen, and D. Nyang, "Catch Me If You Can: Rogue Access Point Detection Using Intentional Channel Interference," in IEEE Transactions on Mobile Computing, vol. 19, no. 5, pp. 1056-1071, 1 May 2020, doi: 10.1109/TMC.2019.2903052