
**ISAR Journal of Science and Technology**

**Volume 3, Issue 1, 2025, Page: 14-18**

*Abbriviate Title- ISAR J Sci Tech*

ISSN *(Online)*- 2584-2056

https://isarpublisher.com/journal/isarjst

# Enhance Threat Detection via Rogue Access Point Monitoring

**Mohamed Adam***

Department of Management Information System, Collage of Business and Economics, Qassim University, Buraydah, Saudi Arabia.

***Corresponding Author**

**Mohamed Adam**

Department of Management Information System, Collage of Business and Economics, Qassim University, Buraydah, Saudi Arabia.

**Article History**

Received: 01.12.2024
Accepted: 25.12.2024
Published: 27.01.2025

**Abstract:** In wireless networks, security measures primarily focus on protecting the privacy and security of end users. Consequently, numerous security risks and threats, especially in public spaces, remain prevalent. Among the most common forms of cybercrime are identity theft and data leaks from university networks. However, users of wireless networks in educational institutions, including universities, often remain unaware of the security risks posed by unsecured networks. This lack of awareness makes users vulnerable to various attacks due to their inexperience or carelessness. This study aims to delve deeper into the dangers associated with fraudulent access points and proposes potential solutions to mitigate this specific category of threats in wireless networks, particularly Rogue Access Points (RAP). Emphasizing RAP among the various potential threats in wireless network systems is justified, as these attacks are highly dangerous and directly affect almost all other common threats in these systems. Once a rogue access point is established, it often becomes a gateway for other threats to infiltrate the network.

**Keywords:** Security, wireless, Rouge Access point, countermeasures.

**Cite this article:**

Adam, M., (2025). Enhance Threat Detection via Rogue Access Point Monitoring. *ISAR Journal of Science and Technology*, *3*(1), 14-18.

## I. Introduction

The widespread worldwide adoption of wireless Internet access can be attributed to its numerous advantages, including better connectivity to information services and greater efficiency. Wireless networks offer simpler, faster and more cost-effective configuration and reconfiguration processes. However, these benefits come with a significant security challenge that can change the current risk profile of information security. The primary vulnerability of wireless networks stems from the use of air and/or radio frequencies for communication, resulting in a higher risk of interference compared to wired networks. This increased risk means that unencrypted messages or messages encrypted with weak algorithms are more susceptible to interception by unauthorized persons, which can compromise privacy. Despite the evolving nature of security threats in wireless networks, basic security priorities remain consistent with those of wired networks. A significant security issue for WLANs is the presence of unauthorized access points (APs) in the network. An unauthorized access point is defined as any active wireless access point that has not been authorized by the WLAN administrator. Malicious users can perform two types of network attacks: passive and active. Passive attacks involve gathering information by simply monitoring network traffic without sniffing or modifying packets, which serves as a preliminary stage before launching the actual attack. Active attacks are more common because the attacker interacts with the victims and can be identified on the network. In these attacks, the perpetrator actively participates in the communication by intercepting and altering the packets exchanged between the parties. Due to the imminent threat potential in wireless network systems, the primary objective of this research is to identify dangerous access point threats and review their countermeasures in wireless network systems. In addition, this study proposes a model for fast and accurate detection of malicious APs in a WLAN environment. This model examines packet frames to determine access point characteristics and compares them to predetermined standards, distinguishing rogue access points from authorized ones.

This research examines a case study based on common security issues encountered with Wi-Fi used in institutional network. Defines WLAN threats and explores in depth the threat of rogue access points. The analysis is then used to develop a potential solution to minimize the rogue access point threat to the systems.

## II. Related Work

The problem of fraudulent access points in wireless networks has become the focus of extensive research. Many researchers have addressed this topic over the years, and this section summarizes previous investigations into the detection of dangerous access point threats. Table 1 offers a comparative analysis of previous research efforts in this area.

## 1. Rogue Access Point Detection Methods: A Review

In [9] aims to explore various techniques for identifying unauthorized access points. These methods are divided into three groups: client-side methods, server-side methods, and hybrid approaches. Each technique has its advantages and limitations. Clients typically have fewer resources and less control over the network compared to servers. Among all the approaches, the hybrid method appears to be the most effective, which reduces the limitations of client-side implementations and at the same time includes server management for rogue access point (AP) detection. The primary contribution of this study is the classification of various Rogue Access Point detection techniques based on their implementation along with recommendations of the most effective methods. In this document, Rogue Access Points are further categorized as wired or wireless depending on their configuration.

## 2. A Measurement-Based Rogue AP Detection Scheme

This paper examines a category of rogue access points (APs) that impersonate legitimate APs to lure users into connecting to them. To help users avoid connecting to rogue APs, a practical timing-based method has been proposed. This approach, independent of WLAN operator assistance, uses the round-trip time between the user and the DNS server to determine the authenticity of the access point. These are the main contributions in this article: (1) A timing-based rogue AP detection algorithm was proposed. Its operation depends only on the current network protocols and can be deployed in any common WLAN without the need for further modifications by the network administrator. Considering a more powerful malicious adversary actively maintaining a rogue AP to escape detection, rather than a "random" rogue AP deployed by, say, an innocent administrative worker. Implementation of a scheme using commercial off-the-shelf wireless cards with real-world testing to assess performance [10].

## 3. Fraudulent access point detection and mitigation

This article focuses on Rogue Access Points, which pose critical security challenges in wireless networks. It examines the most basic and widespread security strategies to address the Rogue Access Point security challenge in wireless networks. This article presents various recent surveys related to rogue access point detection methods or solutions. These surveys were conducted by various researchers, who reported the weak points of a given solution, the level of accuracy of several solutions, and other aspects that affect the detection of fraudulent access points [11].

## 4. A flexible framework for detecting rogue access points

This article provides an overview of the most prevalent and latest types of Wi-Fi threats, so this article discusses the concepts of RAP and types of RAP and some countermeasures. Based on these findings, the RAP detection system was developed to cover the most common attacks. This proposed solution is a modular framework consisting of scanners, detectors, and actuators that are in charge of scanning access points, detecting them using a set of heuristics, and implementing a countermeasure mechanism [12].

## 5. Detection of a rogue client-side access point using a simple walk strategy and round-trip time analysis

In this paper, a technique for detecting rogue APs on the mobile user side is proposed. Using a simple walking method, the round trip time (RTT) and modulation and coding scheme values are obtained, thereby calculating a more accurate bit rate for specific RTT values. Next, the cleaned data is classified using the k-means method and the cumulative distribution function for the detection process. The results show that rogue-APs can be detected with an F-measure as low as 0.9[13].

## 6. Detection And Isolation Of The Remaining Access Point

The main objective of this work is to detect and disable rogue devices in an SDN network, and three techniques are proposed to achieve this objective. The results show that the detection and isolation algorithms are effective. This is understandable since unauthorized users are unable to ping legitimate network users. Furthermore, the scalability and stability of the network is tested by expanding the number of users [14]. 4. Detection and Elimination of Unauthorized Access Points in IEEE-802.11 WLANs Based on Agent Terminology and Distortion Intervals: A Proposal The concept of using a master-slave system to detect and block unauthorized access points in wireless networks has been expanded. Adding clock bias increases efficiency and allows each slave agent to regularly scan not only new access points but also existing access points for any unwanted behavior [15].

## 7. Elimination of Rogue access point in the wireless network

In this paper, a new approach to detect rogue access points has been proposed. The proposed system is a wireless intrusion detection system in the traditional sense of the word. It uses a hybrid approach [16].

## 8. Unauthorized access point detection using network traffic characteristics analysis

This paper describes a method for detecting RAP in a network that consists of wired and wireless subnets. In two parts, the technique is implemented by evaluating traffic characteristics. The first phase highlights the differences in traffic patterns between Ethernet and WLAN. This resolution helps in detecting WLAN hosts. The second phase examines the wireless traffic identified in the first phase to determine whether unauthorized WLAN hosts are connected to the RAP [17].

## 9. Locating an unauthorized access point using subtle channel information

This study used Channel State Information (CSI), which is readily available from commercial Wi-Fi devices, to accurately locate a rogue AP. Only a single off-the-shelf Wi-Fi device is used to locate rogue access points, requiring very little infrastructure. Direction determination and position estimation are two components of the proposed rogue AP localization architecture. The human blocking effect on the amplitude or phase of the CSI can be used to determine the direction of travel. Two approaches are available to determine the location of the rogue AP relative to the estimated direction: calculating directions at several locations based on triangulation and walking toward the rogue AP with direction adjustment. Compared with existing RSS-based approaches, the results of extensive indoor and outdoor trials indicate that our

system can provide more practical and accurate localization of malicious APs [18].

**10. Rogue Access Point Detection: Taxonomy, Challenges and Future Directions.**

This article categorizes known solutions, highlights shortcomings, and recommends future research directions for various RAPs. The goal is to identify existing detection approaches and discover new types of RAPs that have yet to be defined by researchers [19].

TABLE 1: COMPARED METHODS FOR ROGUE ACCESS POINT DETECTION

| Method | Description | Advantages | Limitations |
|---|---|---|---|
| Client-Side Methods | Detection techniques implemented on client devices. | Easy to deploy, no need for network changes. | Limited resources, less control over the network |
| Server-Side Methods | Detection techniques implemented on network servers. | More resources, better network control. | Higher deployment cost, potential network changes required |
| Hybrid Methods | Combines client-side and server-side techniques. | Balances resource usage and control, more effective detection. | Complexity in implementation and maintenance |
| Timing-Based Detection | Uses round-trip time (RTT) between user and DNS server to detect rogue APs. | Independent of WLAN operator assistance, deployable in any common WLAN. | May not detect more powerful malicious adversaries |
| Wireless Fingerprinting | Uses unique characteristics of wireless signals to identify rogue APs. | High accuracy, minimal infrastructure requirement. | Requires specialized equipment and data analysis |
| Traffic Analysis | Analyses network traffic patterns to detect anomalies. | Effective in heterogeneous networks. | Dependent on traffic patterns, may require extensive data collection |
| Channel State Information (CSI) Analysis | Uses CSI to locate rogue APs with high accuracy. | High accuracy, minimal infrastructure requirement. | Requires CSI data and multiple location measurements. |

A comprehensive study was conducted to solve the problem of security threats and risks that are often found in wireless networks, especially in public areas. In this survey shown in Table 1, the researchers used different strategies to overcome the problems. However, while Hao uses Measurement Based Rogue AP Detection to provide the end user with a viable timing-based technique to avoid connecting to rogue Aps Mehndi and others used, he proposed a new approach to detect rogue APs as an intrusion detection system in the traditional sense with a hybrid risk minimization approach. However, Songrit regularly used existing access points for any unwanted behavior.

## III. CURRENT SYSTEM

The university network contains a main router connected to an Internet Service Provider (ISP). This router is connected to the main firewall, which has three legs that connect to three areas: the DMZ, the trusted inside area, and the untrusted outside internet. Inside the DMZ area is a data center that includes a mail server, a web server that includes the university website www.sustech.edu, and an FTP server. A school network is a small internal network that contains a group of access point devices. This network allows students to access internal network services, such as access to school websites and saved lectures, and allows university teachers and official staff to access the Internet with certain restrictions.

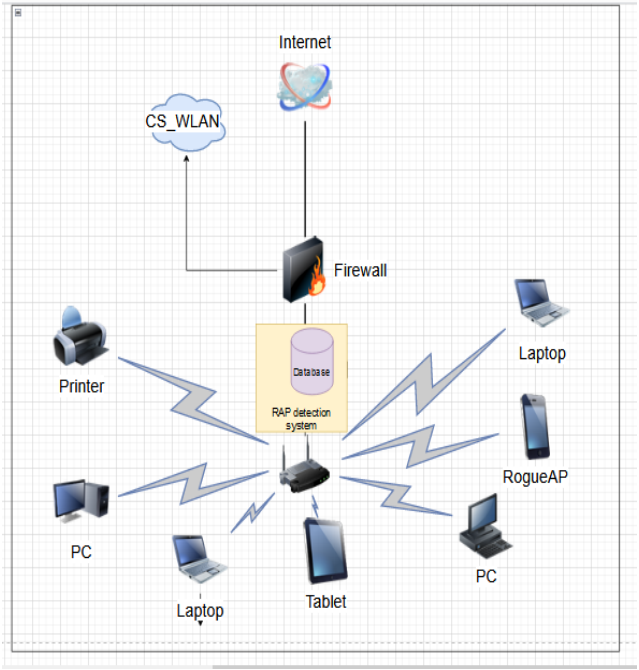


Fig. 1 Current Network Design

## IV. METHODOLOGY

In this research, we study various researchers who have primarily focused on Wi-Fi security and protection techniques using spoofing devices. Although the techniques used in previous studies have been shown to be effective, since we will be conducting this research on a university network, we recommend recording all devices used along with their IP addresses and MAC addresses.

The detection of rogue access points (RAPs) depends on their presence in the WLAN. To monitor the network and determine the presence of a rogue device, the system captures frames and extracts parameters such as MAC addresses. The system then compares the captured parameters with previously stored authorized parameters in the database. If there is a discrepancy, the AP will be classified as rogue. Conversely, if the captured parameters match those of an existing authorized AP, the AP will be classified as authorized.

Next, we will explore a case study based on common security issues encountered with college Wi-Fi. Additionally, we will define WLAN threats and focus in detail on the rogue access point threat. Finally, we will suggest possible solutions to minimize the

threat of fraudulent access points to our systems. In the subsequent section, the results of the proposed network will be presented.

## V. PROPOSED SYSTEM

The system proposed in this research is a rogue WLAN access point detection system designed for network administrators to identify and mitigate rogue devices within the network. This system functions as a gateway to both the local network and the Internet, ensuring comprehensive monitoring and security.

a- System Architecture

The proposed system operates by receiving all packets from connected access points. It captures the MAC addresses and IP addresses of the devices attempting to connect to the network. These captured addresses are then compared with a database of authorized MAC addresses and IP addresses.

b- Detection Mechanism

**Packet Capture**: The system continuously monitors network traffic, capturing packets from all connected access points.

**Address Extraction**: From the captured packets, the system extracts the MAC addresses and IP addresses of the devices.

**Database Comparison**: The extracted addresses are compared against a pre-stored database of authorized MAC addresses and IP addresses.

**Authentication:** If a match is found between the captured addresses and the database entries, the device is considered authorized and allowed to access the network.

If no match is found, the device is flagged as rogue and is denied access to the network.

c- Security Measures

The current network security system enhances this process by assigning each user a unique password to access the network. When a user enters their password for the first time, the system records the device's MAC address and associates it with the user's password. This password is then exclusively used for that specific device, adding an additional layer of security.

## VI. RESULT

**Real-time Detection**: The system provides real-time monitoring and detection of rogue access points, ensuring immediate response to potential threats.

**Enhanced Security**: By associating unique passwords with specific devices, the system prevents unauthorized access even if a password is compromised.

**Scalability:** The system can be scaled to accommodate large networks with numerous devices and access points.

## VII. CONCLUSIONS

In Wireless networks are increasingly popular in homes, offices, and public places like universities, but security remains a major concern. Unauthorized access points (APs) pose significant risks, as they can be exploited by hackers to launch attacks. Network administrators need effective methods to identify and control rogue APs.

In our institution network we uses password authentication, but this alone is insufficient for high security. This study developed a model to detect rogue APs on WLANs, using an experimental research design to test various access points and determine key parameters.

A functional prototype was created using use case diagrams and the C# programming language. The system was tested and successfully identified whether AP beacon frames came from authorized or rogue devices. The developed system is easy to set up and configure, with a user-friendly graphical interface for network administrators.

## VIII. REFERENCES

1. Karygiannis, T., & Owens, L. (2002). *Wireless Network Security:*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.
2. Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017, July). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. In *2017 International Conference on Signal Processing and Communication (ICSPC)* (pp. 288-293). IEEE.
3. Noor, M. M., & Hassan, W. H. (2013). Wireless networks: developments, threats and countermeasures. *International Journal of Digital Information and Wireless Communications (IJDIWC)*, *3*(1), 125-140.
4. Yu, B., & Zhang, L. Y. (2014, November). An improved detection method for different types of jamming attacks in wireless networks. In *The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014)* (pp. 553-558). IEEE.
5. Lu, P. (2020). A position self-adaptive method to detect fake access points. *Journal of Quantum Computing*, *2*(2), 119.
6. Alotaibi, B., & Elleithy, K. (2016). Rogue access point detection: Taxonomy, challenges, and future directions. *Wireless Personal Communications*, *90*, 1261-1290.
7. Thompson A. F. Adebayo, (2016). “detection of wireless rogue access point attack on server systems”,.
8. Anmulwar, S., Srivastava, S., Mahajan, S. P., Gupta, A. K., & Kumar, V. (2014, February). Rogue access point detection methods: A review. In *International Conference on Information Communication and Embedded Systems (ICICES2014)* (pp. 1-6). IEEE.
9. Han, H., Sheng, B., Tan, C. C., Li, Q., & Lu, S. (2009, April). A measurement based rogue ap detection scheme. In *IEEE INFOCOM 2009* (pp. 1593-1601). IEEE.

10. Samra, M., Mengi, M., Sharma, S., & Gondhi, N. K. (2015). Detection and mitigation of rogue access point. *Journal of Scientific and Technical Advancements*, *1*(3), 195-198.

11. Gonçalves, R. J. E. (2017). *A flexible framework for rogue access point detection* (Master's thesis, Universidade do Porto (Portugal)).

12. Kitisriworapan, S., Jansang, A., & Phonphoem, A. (2020). Client-side rogue access-point detection using a simple walking strategy and round-trip time analysis. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), 252.

13. Ampatzi, C. (2021). Detection and Isolation of a Rogue Access Point.

14. Sriram, V. S., Sahoo, G., & Agrawal, K. K. (2010, February). Detecting and eliminating Rogue Access Points in IEEE-802.11 WLAN-a multi-agent sourcing Methodology. In *2010 IEEE 2nd international advance computing conference (IACC)* (pp. 256-260). IEEE.

15. Thite, M. S., Vanjale, S., & Mane, P. B. (2013). Elimination of Rogue access point in Wireless Network. *International Journal of Scientific & Engineering Research*, *4*(12).

16. Shetty, S., Song, M., & Ma, L. (2007, October). Rogue access point detection by analyzing network traffic characteristics. In *MILCOM 2007-IEEE Military Communications Conference* (pp. 1-7). IEEE.

17. Wang, C., Zheng, X., Chen, Y., & Yang, J. (2016). Locating rogue access point using fine-grained channel information. *IEEE Transactions on Mobile Computing*, *16*(9), 2560-2573.

18. Alotaibi, B., & Elleithy, K. (2016). Rogue access point detection: Taxonomy, challenges, and future directions. *Wireless Personal Communications*, *90*, 1261-1290.