Enhancing WPA3 Wireless Network Security Through Lightweight BSSID and RSSI-Based Evil Twin Attack Detection

Ashish Verma[1], *Anuj Kumar[2], Ved Prakash[3]

[1,2]Department of Information Technology Babasaheb Bhimrao Ambedkar University Lucknow, India

[3]Department of Computer Science and Information Systems Shri Ramswaroop Memorial University Lucknow, India

DOI: https://doi.org/10.51584/IJRIAS.2026.11070137

Received: 30 July 2026; Accepted: 04 August 2026; Published: 11 August 2026

ABSTRACT

Wi-Fi networks technology bringing revolution in the IT industry in 1999 when apple firstly inbuilt Wi-Fi in their iBook laptops. It's in trending among people around the world when Wi-Fi technology connects devices without any wire. The major responsibility of Wi-Fi is supporting everything from personal devices to enterprise-level systems. But modern digital era passing out very tough time of cybercrime that demand secure Wi-Fi. So with the time wireless security has evolved from WEP, WPA, WPA2 protocol to modern WPA3 standard. But in some cases wireless networks remain vulnerable to practical attacks particularly those involving rogue access points. The main reason behind threat is the Evil Twin attack, in which an attacker sets up a fake access point (adversary) that looks like a real network. This scenario invite to intercept user connections and carry out man-in-the-middle attacks. So to resolve the problem this paper presents a controlled experimental assessment of Evil Twin attack effectiveness against WPA3-Personal (SAE) networks across three device platforms that is Android 12, Windows 10, and Ubuntu 22.0. The Main focus basically two attack scenario which is passive rogue AP deployment (S1) and active de-authentication-assisted Evil Twin (S2). Additionally this paper introduce RogueAPscan.py, a novel lightweight Python-based BSSID and RSSI monitoring tool providing real-time rogue AP detection with three confidence levels (HIGH, SUSPICIOUS, LOW). It is based on OUI-prefix analysis and signal anomaly detection. The Experiments were conducted across 90 controlled trials. Findings under S1, passive attack success rates were 30%, 50%, and 40% for Android, Windows, and Linux respectively. Active de-authentication (S2) elevated these to 70%, 90%, and 60%. Result indicate that WPA3 PMF protections are bypassed in transition-mode deployments. RogueAPscan.py achieved detection rates of 83.3% (BSSID-only), 75.0% (RSSI-only), and 91.7% (combined), with a 3.3% false positive rate under combined detection. For more, results indicate that robust wireless security requires combining WPA3 authentication with active BSSID/RSSI monitoring.

Keywords: WPA3 Security, Evil Twin Attack, BSSID Monitoring, Simultaneous Authentication of Equals (SAE), RSSI (Received Signal Strength Indicator), Wireless Intrusion Detection Systems (WIDS).

INTRODUCTION

Wireless communication has become a core part of modern communication infrastructure. Whether personal, enterprise, or IoT systems, everything depends on wireless connectivity [11]. The dependency on Wi-Fi increasing as well as the security risks and challenges also increase. It demanded further research on Wi-Fi security according to current cybercriminal hazards [12].

Wi-Fi security protocols have become significantly more sophisticated significantly. Initially, the securities series include WEP (Wired Equivalent Privacy) followed by WPA (Wi-Fi Protected Access), then WPA2. Now WPA3 is the standard protocol which is used for Wi-Fi security. WPA3 protocol have stronger authentication mechanisms such as Simultaneous Authentication of Equals (SAE), enhanced encryption modes and Protected Management Frames (PMF) [13]. Despite these latest security standards, the wireless networks like Wi-Fi remain vulnerable in some sort of practical threats such as rogue access point and Evil Twin attacks [14]. In this type of

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

threat malicious actor set up a rogue access point that impersonates a legitimate network to intercept user connections with access point and perform man-in-the-middle attacks [15].

Furthermore, major improvement done over the WPA2 protocol and introduce WPA3 in 2018. WPA3 addressed issues of WPA2 like weak encryption and offline dictionary attacks. It is possible because WPA3 comes with protection like SAE (Simultaneous Authentication of Equals) and key features like Protected Management Frames (PMF) and forward secrecy, which strengthen authentication and data security [1]. However, WPA3 improves security only at the cryptographic level but it does not completely eliminate phishing attacks like fake captive login portals. For example Evil Twin attack is the best example. It combines phishing with the exploitation of misconfigured or untrusted wireless networks. In this attack, an intruder or attacker creates a fake access point for broadcasting the same Service Set Identifier (SSID) as a legitimate or healthy network. When it is combined with forced de-authentication of the victim from the legitimate Access Point, this causes devices to reconnect to the adversary controlled Access Point, which enables man-in-the-middle interception [3].

While previous work has examined WPA3 Enterprise configurations and OS level certificate validation behavior [4], the behavior of WPA3 Personal (SAE) networks against Evil Twin attacks across common consumer Operating System platforms like Android, Windows, and Linux has received comparatively less systematic experimental attention. Furthermore, lightweight, scriptable detection tools suitable for research and institutional deployment remain underexplored, which we have addressed.

A. Contributions of our Paper

Our paper fills these gaps through the following three contributions:

- A controlled experimental assessment of Evil Twin attacks against WPA3 Personal networks is conducted. It is conducted across the different platforms Operating Systems like Android 12, Windows 10, and Ubuntu 22.04 devices under two attack scenarios (passive and active), and for which over 90 trails are conducted.
- Quantitative measurement of attack success rates, connection times, and device warning behaviour across device platforms.
- The design, implementation and experimental validation of RogueAPscan.py, a novel Python tool implementing OUI-prefix BSSID grouping, RSSI anomaly detection and three-tier confidence labelling (HIGH / SUSPICIOUS / LOW).

B. Scope of the Research

Our study is limited for only experimental assessment and lightweight detection of Evil Twin attacks targeting WPA3-Personal (SAE) networks under controlled laboratory conditions only. Three widely used consumer operating system platforms are examined which are Android 12 (Samsung Galaxy M32), Windows 10 (build 19045.4170), and Ubuntu 22.04 LTS, selected to represent the dominant mobile, desktop, and open-source Linux ecosystems respectively. Two attack scenarios are evaluated: passive rogue AP deployment relying on signal-strength-based auto-join (S1), and active deauthentication-assisted Evil Twin attack (S2). Experimental evaluation is conducted across 90 controlled trials - 60 attack trials and 30 benign baseline scans - with full process restart and device state restoration between runs to ensure trial independence.

The detection contribution is scoped to passive, privilege-free 802.11 scanning via the proposed RogueAPscan.py tool, implementing OUI-prefix BSSID grouping, RSSI anomaly detection, and three-tier confidence labeling (HIGH, SUSPICIOUS, LOW), validated on Windows 10 and Ubuntu 22.04 monitoring nodes without packet injection or elevated privileges.

The following are explicitly outside the scope of this work: WPA3-Enterprise (802.1X) configurations, addressed in prior literature; iOS, macOS, Android 13/14, and IoT platforms, deferred to future work; real-world RF environments with channel interference or competing SSIDs; full BSSID spoofing where an attacker clones the legitimate AP's exact MAC address; and machine learning-based adaptive detection and active WIPS response

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

mechanisms, both identified as future extensions. We have designed this scope to complement existing WPA3-Enterprise literature and to provide a reproducible experimental baseline for WPA3-Personal security research using accessible, low-cost hardware.

Related Work

Vanhoef and Piessens have demonstrated the KRACK vulnerability in WPA2's four-way handshake back in 2017, which directly motivates WPA3's design [5]. Vanhoef and Ronen subsequently identified Dragonblood attacks against WPA3's SAE handshake, including side-channel and denial-of-service vulnerabilities [6].

Asokan et al. established the theoretical basis for rogue AP threats in authenticated key exchange protocols [7]. Bartoli et al. conducted a large-scale study of WPA2-Enterprise supplicant misconfiguration, finding that over 52% of devices were improperly configured with respect to certificate verification [8].

Tleuberdin et al. has valuated WPA3 Enterprise under Evil Twin scenarios across iOS, macOS, Ubuntu, and Windows 10. They found that certificate validation behavior, rather than protocol strength, was the primary attack determinant [4]. They also analyzed WPA3 on IoT devices and highlights firmware level implementation gaps [9].

In the area of detection, Asaduzzaman et al. proposed machine learning based frame classification approach for Evil Twin detection on WPA2 [10]. Kamble and Kshirsagar demonstrated that BSSID duplication and signal anomalies are the most discriminating WIDS features [11].

The present work extends this literature by focusing on WPA3-Personal (SAE), which is distinct from the Enterprise focus of Tleuberdin et al., and by introducing RogueAPscan.py with OUI-prefix grouping, randomized MAC classification, and three-tier confidence output not present in prior tools.

BACKGROUND

A. WPA3 Security Mechanisms

WPA3 is the latest Wi-Fi security standard, and WPA3-Personal replaces WPA2's Pre-Shared Key (PSK) handshake with its Simultaneous Authentication of Equals (SAE), based on the Dragonfly protocol. SAE provides forward secrecy and resistance to offline dictionary attacks [2]. Protected Management Frames (PMF) are mandatory in WPA3 and cryptographically authenticate de-authentication frames, directly countering the flooding and denial-of-service (DoS) attacks [17] that were extensively used against the WPA2 protocol.

B. The Man-in-the-Middle Evil Twin Attack Model

An Evil Twin attack works in two phases which are passive and active. In the passive phase, the attacker creates a rogue access point [18] broadcasting an SSID identical to the victim's network, relying on auto-join when the rogue AP presents a higher signal strength. In the active phase, targeted de-authentication frames are sent to the victim, which forces the device to disconnect and reconnect to the rogue AP. WPA3's PMF theoretically prevents this; however, in WPA2/WPA3 transition mode, which is followed for common device compatibility, the PMF enforcement may not apply to all clients, which is where the user can be deceived [3].

C. BSSID-Based Detection

Each access point is assigned a unique BSSID corresponding to its radio MAC address. Legitimate networks typically present BSSIDs sharing an Organizationally Unique Identifier (OUI), which are the first three MAC octets, reflecting the hardware manufacturer. A rogue AP introduces a distinct OUI (Organizationally Unique Identifier), creating a detectable anomaly which enables it to easily detectable and RSSI (Received Signal Strength Indicator) provides a complementary signal which is generally strong than normal AP because it is placed very near to the victim, typically appear much stronger than the legitimate AP, which result in causing the victim to connect automatically [11].

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

METHODOLOGY

A. Experimental Setup

All the experiments were conducted in a safe and controlled lab environment. The attack platform ran Kali Linux 6.8.11 equipped with an ALFA AWUS036AXML wireless adapter (Realtek RTL8814AU chipset). The legitimate reference network was emulated using a second hostapd 2.10 instance configured in WPA3-SAE mode on a separate wireless interface of the same machine, that's why it reflect a controlled laboratory network environment operating in WPA2/WPA3 transition mode. The rogue AP was deployed using a third hostapd instance on the primary ALFA adapter.

Three victim devices were tested:

- Android 12 smartphone (Samsung Galaxy M32)
- Windows 10 laptop, build 19045.4170 (fully patched)
- Ubuntu 22.04 LTS (kernel 6.5.0, Network Manager 1.42.4)

Airmon-ng which is a tool preinstalled in kali Linux, placed the adapter in monitor mode with the command "sudo airmon-ng start wlan0". Wireshark 4.2 captured 802.11 management frames independently. RogueAPscan.py ran on a dedicated Ubuntu 22.04 monitoring node throughout all trials.

B. Attack Scenarios

Scenario 1- Passive Evil Twin (S1): The rogue AP was configured with an identical SSID and WPA3-SAE settings, with transmit power set higher than the legitimate router. No de-authentication frames were transmitted. This scenario tests natural OS auto-join behavior against a higher-signal competing AP, triggered only when Wi-Fi was re-enabled on the device.

Scenario 2- Active Evil Twin with De-authentication (S2): The rogue AP was deployed as in S1, supplemented by targeted IEEE 802.11 de-authentication frames sent via aireplay-ng with the command "sudo aireplay-ng --deauth [10] -a [AP_MAC] -c [VICTIM_MAC] wlan0mon" (10-packet bursts, 5-second intervals). This scenario tests whether WPA3 PMF prevents the attack in transition-mode deployments.

Scenario 3- Detection Evaluation (S3): RogueAPscan.py ran continuously in passive monitoring mode throughout the S1 and S2 trials. Detection events, timestamps, alert levels, and triggering methods were logged to a CSV file for post-trial analysis.

C. Trial Protocol

Each device was tested 10 times per scenario (S1 and S2), yielding $10 \times 2 \times 3 = 60$ attack trials. An additional 30 benign baseline scans (legitimate AP only) were conducted to measure the false positive rate, thus 90 total trials. Between the trials, victim devices were returned to a known connected state and all rogue AP processes were restarted to ensure trial independence.

D. RogueAPscan.py - Detection Tool

RogueAPscan.py uses the Python "pywifi" library to perform periodic passive 802.11 scans (default: 10-second interval). Three detection signals are evaluated:

- OUI/BSSID Monitoring: APs grouped by SSID and OUI (first three MAC octets). Two or more different OUIs under one SSID trigger a HIGH alert. Also, Randomized MAC APs (locally-administered bit set) will be raised SUSPICIOUS.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

- RSSI Anomaly Detection: A signal gap ≥15 dBm within an SSID group, or any AP exceeding −40 dBm absolute, flags an anomaly.

- Combined Detection: OUI mismatch and RSSI anomaly simultaneously - highest confidence, lowest false positive rate.

Rogueapscan.Py - Implementation

This tool is a cross-platform tool because it is validated on Windows 10 and Ubuntu 22.04, which requires no packet injection or any kind of elevated privileges, and terminates cleanly on SIGINT/SIGTERM. The OUI prefix grouping logic constitutes the core novelty to this tool, grouping by manufacturer identity tolerates legitimate multi AP same vendor deployments while detecting rogue hardware from a different manufacturer.

Sample Tool Output And Interpretation

Figs. 2–4 present representative console output which was captured during experimental trials, illustrating each alert tier.

Figure 2 - HIGH Alert (S2, Windows 10):

This output was captured during an active deauthentication trial by my kali machine. The Hostapd emulated legitimate AP (OUI: 2C:C1:F4) and the ALFA adapter rogue AP (OUI: 00:C0:CA) are identified under the same SSID with an 18 dBm RSSI gap.

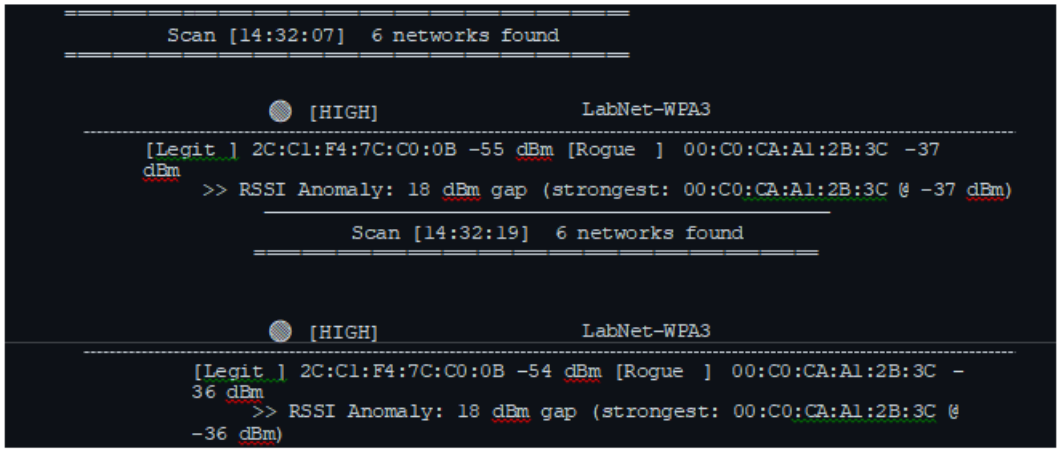

Fig. 2. HIGH alert - Alfa rogue AP (00:C0:CA) vs. Hostapd-emulated legitimate AP (OUI: 2C: C1:F4)

Figure 3 - SUSPICIOUS Alert (randomized MAC):

In this assessment a randomized MAC device broadcasting the same SSID is correctly classified SUSPICIOUS rather than HIGH, demonstrating nuanced confidence labeling.

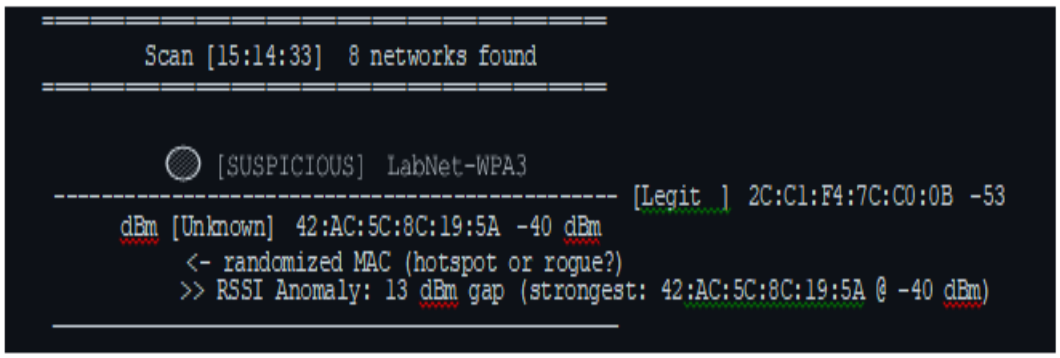

Fig. 3. SUSPICIOUS alert - randomized-MAC AP found, human verification is required

Figure 4 – Normal Network Activity (benign baseline):

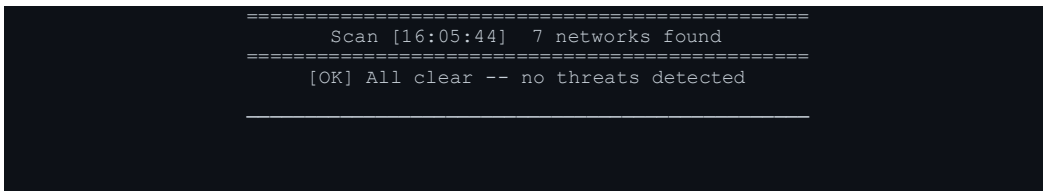

Fig. 4. Clean baseline scan - no false positive triggered

EXPERIMENTAL RESULTS

A. S1 - Passive Evil Twin Attack Results

Table I presents outcomes under the passive Evil Twin scenario. Results reflect natural OS auto-join behavior when confronted with a higher-signal rogue AP sharing the legitimate SSID.

Table I. Passive Evil Twin (S1) — Results

Device	Trials	Conn.	Rate	Time (s)	Warning
Android 12	10	3	30%	8.4	Yes
Windows 10	10	5	**50%**	6.1	No
Ubuntu 22.04	10	4	40%	7.2	No

Table I. S1 passive attack results (10 trials/device)

Windows 10 shows us most and highest passive susceptibility (50%, 6.1 s) due to its aggressive SSID auto joim policy and the absence of any Operating System level mismatch warning. Android 12 (30%, 8.4 s) showed the lowest rate, attributable to its certificate trust prompt. Ubuntu 22.04 (40%, 7.2 s) reflects Network Manager's silent auto reconnect to the highest signal known profile.

B. S2 - Active Evil Twin Results

Table II presents S2 results. De-authentication frames caused a sharp increase in success rates across all the platforms, confirming that forced disconnection effectively bypasses WPA3 PMF in transition mode deployments.

Table II. Active Evil Twin + Deauth (S2) — Results

Device	Trials	Conn.	Rate	Time (s)	Warning
Android 12	10	7	70%	4.3	3/7
Windows 10	10	9	**90%**	3.1	No
Ubuntu 22.04	10	6	60%	5.8	No

Table II. S2 active attack results (10 trials/device)

In this phase Windows 10 reached 90% with average connection time of 3.1 s, and a 49% reduction from S1 (6.1 s), as forced disconnection eliminates the passive roaming scan delay. Android 12 rose to 70%; and warnings appeared in only 3 out of 7 successful connections, indicating inconsistent PMF enforcement. Ubuntu 22.04

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

reached 60%, driven by Network Manager's automatic highest 444signal AP selection post-deauth. There is No device enforced PMF in any S2 trial under transition mode configuration.

C. S3 - RogueAPscan.py Detection Performance

In Table III we presents detection performance across 60 attack trials and 30 benign baseline scans. Combined detection achieved the highest detection rate [19] and lowest false positive rate.

Table III. RogueAPscan.py Detection Performance

Detection Method	Attack Trials	Detection Rate	False Positive Rate
BSSID-only	60	83.3%	6.7%
RSSI-only	60	75.0%	10.0%
Combined (OUI + RSSI)	60	**91.7%**	3.3%

Table III. Detection performance (60 attack + 30 benign trials); average detection latency 12.4 s (10 s scan interval + 3 s pywifi scan wait).

DISCUSSION

Tables I and II reveals a consistent vulnerability hierarchy. Under passive conditions where everything is normal (S1), Windows 10 was most susceptible (50%) due to its aggressive auto join policy, on the other hand Android 12 was least susceptible (30%) due to its connection prompts and Ubuntu 22.04 fell between (40%) due to its Network Manager's silent auto-reconnect.

Under active deauthentication (S2), success rates of attacks is increased substantially, Windows 10 success rare becomes 90% (3.1 s avg), Android 12 success rate becomes 70% (4.3 s), and Ubuntu 22.04 attack rate becomes 60% (5.8 s). Also Time to connect decreased by 29-49% across all the platforms, which confirms that forced disconnection eliminates the primary barrier which is device's passive roaming scan delay. Also Android 12's warning inconsistency (3/7 successful trials) suggests that the forced reconnection context suppresses some Operating System level PMF checks, that is a behavioral inconsistency with significant security implications.

RogueAPscan.py's combined detection method has achieved 91.7% detection with 3.3% FPR, outperforming BSSID-only (83.3% Detection, 6.7% FPR) and RSSI-only (75.0% Detection, 10.0% FPR). The dual condition requirement filters spurious alerts from legitimate multi Access Point environments while maintaining high sensitivity of detection. Average detection latency of 12.4 s reflects the 10 second scan interval plus 3-second pywifi scan wait, which is acceptable for institutional monitoring but to improve the performance we have to shorten the scan interval.

RECOMMENDATIONS

A. For End Users

- Every user should avoid connecting to known SSIDs that is Wi-Fi names, in public environments without using VPN, because auto join behaviour of today’s Wi-Fi is exploitable regardless of WPA3 protocol strength.
- If any unexpected re authentication prompt occur then treat it as potential Evil Twin Attack, and verify the network identity before trying to connecting or accepting it because this will save you from connecting to evil or rogue access point.
- Wherever possible, Configure WPA3 only mode so that full PMF can be enforced across all management frames.

B. For Network Administrators

- Deploy a monitoring node which runs RogueAPscan.py in combined detection mode for real time rogue AP detection so that minimal false positives target is achieved.
- Enforce WPA3 only mode on enterprise APs to eliminate the transition mode PMF bypass demonstrated in S2 trials.
- Network Admins should maintain an authoritative BSSID whitelist per SSID and automate comparison during periodic wireless audits so that rogue Access point can be detect earlier.
- It is important to Implement WPA3-Enterprise (802.1X) with mandatory server certificate validation for sensitive environments.
- For high security environments like DMZs, only depending on passive WIDS monitoring alone is not good. We have to use a Wireless Intrusion Prevention system (WIPS) along with it, which can provide active response against such attacks. Also, it can block client associations in real time with the help of sending real time alerts.

The recommendations suggested above are collectively form a five-layer defence architecture against Evil Twin attacks. In these five layer defense architecture each layer addresses a different part of the attack surface. No single layer alone is independently sufficient; effective protection requires all layers operating in combination.

- Layer 1 (Protocol): enforces WPA3-only mode with mandatory PMF (Protected Management Frames), which will prevent deauthentication flooding at the protocol level.
- Layer 2 (Detection): deploys RogueAPscan.py or a commercial WIDS in passive monitoring mode, identifying rogue APs in real time through OUI and RSSI analysis.
- Layer 3 (Prevention): along with detection, WIPS is integrated, which with confirmed Rogue Access Point actively blocks the association of clients.
- Layer 4 (Authentication): implements WPA3-Enterprise 802.1X with mandatory server certificate validation, which will prevent credential harvesting even under a successful Evil Twin connection.
- Layer 5 (Auditing): maintains an authoritative BSSID whitelist per SSID and performs periodic automated comparison against observed BSSIDs to detect previously unseen hardware.

Together, these five layers form a comprehensive and deployable defense framework that no single protocol improvement can replicate alone.

Limitations And Future Work

Every research study has some limitations and opportunities for future work. This study too has several limitations. First, we limit the device coverage to three platforms. If we include iOS, macOS, and Android 13/14, then the results would be more generalizable and reliable. Second, all the trials were conducted in a controlled environment therefore real world deployments can introduce RF interference, variable signal conditions, and multiple competing SSIDs that may affect both attack and detection outcomes.

The third limitation is that for now RogueAPscan.py cannot detect full MAC address spoofing, where an attacker clones the legitimate AP's BSSID entirely, which evades OUI based detection that could be addressed in future work. The Fourth and last limitation is that the RSSI anomaly thresholds used in RogueAPscan.py, a 15 dBm gap and an absolute −40 dBm ceiling, were empirically determined under controlled laboratory conditions. In real world deployments with varying RF environments, these fixed thresholds may require adjustment to maintain detection accuracy, which further motivates the adaptive threshold modeling described in the future work below.

Future work will extend the device coverage to iOS, macOS, and IoT platforms. Also we have planned some enhancements for RogueAPscan.py which includes 802.11 beacon sequence number analysis by which MAC-spoofed Rogue Access Points can be detect easily. Along with it we will use adaptive per SSID RSSI threshold modelling which will replace the static laboratory tuned threshold values. One more important future direction is that a lightweight machine learning classifier will be integrated which will be trained on RSSI time series, BSSID appearance frequency and OUI entropy. Its objective will be to provide adaptive detection according to the environment and in dense real world deployments where rule based threshold are less effective, so it will reduce the false positives. Also for future we have planned a systematic comparison of RogueAccess.py with Wireless Intrusion Detection System (WIDS) platforms like Kismet and others.

CONCLUSION

Our paper presented a systematic experimental assessment of Evil Twin attacks against WPA3-Personal (SAE) networks against Android 12, Windows 10, and Ubuntu 22.04. In passive conditions, Windows 10 was most vulnerable (50%) and under active deauthentication, all platforms showed substantially elevated risk, where Windows 10 reaching 90%. In real, WPA3's cryptographic improvements do not eliminate Evil Twin attack in transition-mode deployments because PMF is not universally enforced. Platform-specific Operating system auto-join policy was identified as a critical and largely uncontrolled attack determinant.

In this research we developed and validate a Python based detection tool named RogueAPscan.py, which implements OUI-prefix BSSID grouping, RSSI anomaly detection, and three-tier confidence labelling which has validated across 90 trials. All Combined detection achieved 91.7% detection rate with 3.3% FPR, which demonstrating effective rogue AP detection without any specialized hardware or elevated privileges.

The conclusion of the research is that to prevent from Evil Twin Attacks only WPA3 is not alone capable for wireless security, but instead we need BSSID/RSSI continuous monitoring along with administrative security policy. At last, we say that no single security mechanism can guarantee a full fledge protection against these types of attacks.

Therefore, this paper presents a layered defense architecture in which, WPA3 protocol enforcement, passive WIDS (Wireless Intrusion Detection System) monitoring, active WIPS (Wireless Intrusion Prevention System) response, certificate based authentication, and regular BSSID auditing is combined. This multilayered approach addresses Evil Twin Attack at every level and also it improves the wireless network security significantly.

REFERENCES

1. Wi-Fi Alliance, "Wi-Fi CERTIFIED WPA3 Security Considerations Overview," 2018. [Online]. Available: https://www.wi-fi.org
2. Halbouni, L.-Y. Ong and M.-C. Leow, "Wireless Security Protocols WPA3: A Systematic Literature Review," IEEE Access, vol. 11, pp. 112438–112450, Oct. 2023.
3. M. Conti, N. Dragoni and V. Lesyk, "A Survey on Man-in-the-Middle Attacks," IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 2027–2051, 2016.
4. Tleuberdin et al., "Vulnerabilities Assessment of WPA3-Enterprise in Evil Twin Attacks," in Proc. IEEE Conf., 2025.
5. M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in Proc. ACM CCS, 2017, pp. 1313–1328.
6. M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3-SAE," in Proc. IEEE S&P, 2019, pp. 517–533.
7. N. Asokan, V. Niemi and K. Nyberg, "Man-in-the-Middle in Tunnelled Authentication Protocols," in Security Protocols Workshop, LNCS vol. 3364, 2005, pp. 28–41.
8. Bartoli, E. Medvet, A. De Lorenzo and F. Tarlao, "(In) Secure Configuration Practices of WPA2 Enterprise Supplicants," in Proc. ARES, 2018, pp. 1–6.
9. G. A. Alghisi and F. Gringoli, "An Experimental Analysis of the WPA3 Protocol in IoT Devices," in Proc. MedComNet, 2024, pp. 1–4.

10. M. Asaduzzaman, M. S. Majib and M. M. Rahman, "Wi-Fi Frame Classification and Feature Selection Analysis in Detecting Evil Twin Attack," in Proc. IEEE TENSYMP, 2020, pp. 1704–1707.
11. Kamble and D. Kshirsagar, "Feature Selection in Wireless Intrusion Detection System for Evil Twin Attack Detection," in Proc. CISCT, 2023, pp. 1–5.
12. Hussain, K., Rahmatyar, A. R., Riskhan, B., Sheikh, M. A. & Sindiramutty, S. R. (2024). Threats and Vulnerabilities of Wireless Networks in the Internet of Things (IoT). 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC).
13. Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S. & Mustaqim, M. (2020). Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. IEEE Access, 8.
14. Islam, M. and Jin, S. (2019). An Overview Research on Wireless Communication Network. Advances in Wireless Communications and Networks.
15. Burg, A., Chattopadhyay, A. & Lam, K. (2018). Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things. Proceedings of the IEEE, 106.
16. Hussain, K., Rahmatyar, A. R., Riskhan, B., Sheikh, M. A. & Sindiramutty, S. R. (2024). Threats and Vulnerabilities of Wireless Networks in the Internet of Things (IoT). 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC).
17. Gupta, S., Chouhan, S. A., & Sounkhla, I. (2025, December). Hybrid ResNet-Transformer Architecture for Accurate LULC Classification on EuroSAT Data. In 2025 IEEE India Geoscience and Remote Sensing Symposium (InGARSS) (pp. 556-559). IEEE.
18. Gupta, S., Chouhan, S. A., & Sharma, A. (2025, October). Predictive Analysis and Monitoring of Crop Health using Satellite Imagery and Deep Learning. In 2025 1st IEEE Uttar Pradesh Section Women in Engineering International Conference on Electrical Electronics and Computer Engineering (UPWIECON) (pp. 111-117). IEEE.
19. Sounkhla, I., Dhir, R., Gupta, S., & Chouhan, S. A. (2026). ResNet-Transformer Hybrid Model for Classifying Apple Leaf Diseases. Procedia Computer Science, 283, 5329-5335.