International Journal of Safety and Security Engineering
Vol. 16, No. 4, April, 2026, pp. 799-813
Journal homepage: http://iieta.org/journals/ijsse

Mathematical Modeling and SDN-Driven Defense for Wi-Fi MAC-Layer Vulnerabilities in Access Points

Farah Natiq Qassabbashi[1], Qutaiba I. Ali[1], Farhad E. Mahmood[2*]

[1] Computer Department, College of Engineering, University of Mosul, Mosul 41002, Iraq
[2] Department of Communications and Intelligent Digital Systems, College of Engineering, University of Mosul, Mosul 41002, Iraq

Corresponding Author Email: farhad.m@uomosul.edu.iq

https://doi.org/10.18280/ijsse.1604xx

Received: 15 March 2026
Revised: 19 April 2026
Accepted: 25 April 2026
Available online: 30 April 2026

Keywords:
Software-Defined Networking, WPA3, MAC address spoofing, MAC address flooding, Key Reinstallation Attack, spanning, IEEE 802.11 WLAN, Evil Twin Rogue access point, deauthentication denial-of-service attacks

ABSTRACT

In IEEE 802.11-based wireless networks, every device is uniquely identified by a Media Access Control (MAC) address. However, these identifiers can be easily spoofed to launch various attacks, including MAC address spoofing, flooding, Key Reinstallation Attacks (KRACK), Spanning Tree Protocol (STP) manipulation, Evil Twin Rogue access point (AP), and deauthentication denial of service (DoS) attacks. Although WPA3 introduces enhancements such as Simultaneous Authentication of Equals (SAE) and Protected Management Frames (PMF) to secure management frames, it remains focused on prevention and lacks real-time detection or mitigation mechanisms, leaving access points exposed during active attacks. This paper proposes a unified security framework based on Software-Defined Networking (SDN) and deterministic mathematical models to defend Wi-Fi access points at the MAC layer. The framework enables real-time detection of malicious behavior using lightweight equations applied to frame-level metadata such as RSSI, sequence numbers, nonces, and authentication rates. By leveraging SDN's centralized control and dynamic flow management, the proposed system enhances WPA3 by adding a scalable and explainable detection layer that improves response time and restores throughput to near-native levels during attacks. This work is further framed as a cross-layer communications model in which MAC-layer attacks are interpreted as disturbances to channel access, frame exchange reliability, and service continuity in IEEE 802.11 WLANs.

1. INTRODUCTION

The expansion of Wi-Fi technology has become substantial within the last few years. Wireless technologies include Wi-Fi, Bluetooth, satellite communication, wireless sensor networks, and more, which provide users with unbroken connectivity at their residences and workplaces and public access spots during transit without requiring cable infrastructure. Any signals transmitted by a Wi-Fi network over airwaves are vulnerable to interception by attackers who remain within a few meters of the Wi-Fi access point (AP). Wi-Fi networks experience multiple possible security attacks. The main cause of numerous Wi-Fi network attacks stems from basic vulnerabilities in the 802.11 protocol. So, a fundamental driver of IoT and mobile cloud computing will experience multiple security attacks due to the security failures of Wi-Fi networks [1].

The use of structured frameworks called layered architectures provides a reliable networking system for communication. The Transmission Control Protocol/Internet Protocol (TCP/IP) suite stands as one of the most frequently used models because it delivers standardized communication procedures between devices. The application and transport, along with network and data link, and physical layers, are the five levels within the TCP/IP model for handling specific data transmission functions. The multilevel organization makes networks more modular and simplifies network troubleshooting and development [2]. The illustration of TCP/IP model architecture can be found in Figure 1. Devices within networked systems communicate via several kinds of address types, such as Media Access Control (MAC) (physical), IP (logical), and port numbers. Each one has a unique function, but there are risks to security involved as well. The attackers may use these addresses to attack devices, compromise network defenses, or interrupt communication.

According to the IEEE 802.11 standard of wireless networking, there are three primary frame categories: management, control, and data frames. Malicious actors are prone to spoofing control and management frames since they lack the encryption and authentication capabilities that data frames have. Attackers can use this vulnerability to impersonate, reduce resource, and media access attacks, among others, which fall under denial-of-service (DoS) attacks. Control frames, such as Acknowledgment (ACK), Request to Send (RTS), and Clear to Send (CTS), and management frames, such as Beacon, Probe

Request/Response, Authentication, Association Request/Response, and Deauthentication/Disassociation frames, are especially vulnerable to spoofing. Therefore, these frames are a great security concern in wireless networks [3].

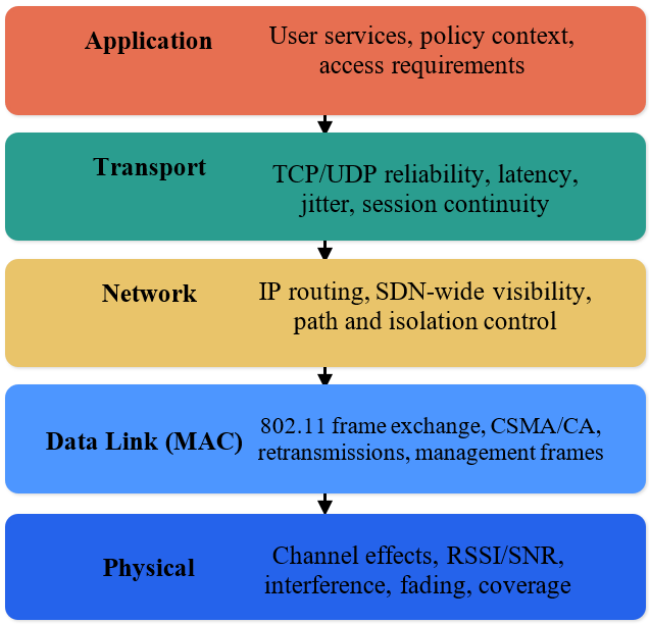

Figure 1. Communication-oriented Transmission Control Protocol/Internet Protocol (TCP/IP) model for IEEE 802.11 WLAN security

From a communications perspective, MAC-layer attacks degrade the reliability and efficiency of wireless medium access by increasing collision likelihood, interrupting association continuity, and distorting PHY/MAC observables such as RSSI and frame timing.

Information security, in particular, in Wi-Fi networks, is becoming more important as the volume of data stored and transmitted through networks continues to grow ever-increasingly. Meanwhile, most of the security processes and means of detecting threats that are currently being employed are no more effective, or are even weaker than before, as a result of technological enhancements. The difficulty of detecting attacks in Wi-Fi networks continues to be a significant and urgent problem due to the increasing number and sophistication of attacks, which are harder to detect and prevent [4]. For as long as such vulnerabilities exist, attackers may use them to interfere with network availability, compromise data integrity, or access sensitive information with no authorization. Spanning tree protocol (STP) manipulation, MAC address spoofing, MAC address flooding, Key Reinstallation Attacks (KRACKs), Evil Twin Rogue access point (AP), and deauthentication DoS attacks are examples of common MAC-layer attacks. These attacks are challenging to detect and mitigate by using conventional techniques because they frequently target the MAC layer's unauthenticated control and management frames.

The impact of traditional defenses, including Wi-Fi PROTECTED ACCESS 2 (WPA2) and WPA3 encryption, static filtering rules, or basic intrusion detection systems, can often be constrained. Most among them have been designed to just handle a single type of attack, primarily depending on human configuration, or need for firmware and hardware changes that are impractical for legacy systems. The vast majority of the existing solutions have failed to adapt to the evolving requirements of a contemporary Wi-Fi setting and lack real-time detection. Moreover, Simultaneous Authentication of Equals (SAE) and a four-way handshake are two significant encryption and authentication methods developed by WPA2 and WPA3. However, their primary focus is on data secrecy, and they have not proven very effective at tackling dynamic, real-time threats at the MAC layer. They are insufficient for adaptive, broad-spectrum attack mitigation in dynamic wireless environments due to their static nature and dependence on firmware updates or strict device compliance. To address these challenges, this paper proposes a unified security framework that leverages the programmability of Software-Defined Networking (SDN) and the transparency of mathematical detection models. The system can be used to implement effective real-time mitigation of various attack types by changing the logic of control to a centralized SDN controller and performing rule-based detection algorithms on the traffic at the MAC layer. This framework accommodates both traditional and current Wi-Fi deployments and is not dependent on machine learning and black-box detection engines; thus, it is lightweight, explainable, and scalable.

The main contributions of this paper: (1) A unified SDN-based security framework for Wi-Fi MAC-layer protection is proposed. (2) A deterministic mathematical detection model is developed for multiple MAC-layer attack types. (3) Attack-specific detection indicators are defined using frame-level metadata available at the AP. (4) It complements WPA3 by adding centralized real-time detection and response capabilities; and (5) MAC-layer attacks are interpreted as disturbances to channel access, frame exchange reliability, and service continuity in IEEE 802.11 WLANs.

The paper is organized as follows: Section 2 shows the background on the MAC layer and SDN. Section 3 presents related work in the MAC-layer attack. In Section 4, the threat model is presented, and in Section 5, the security model. The details of the proposed security model are described in Section 6, and the expected results and system behaviour are discussed. Section 7 presents a comparative analysis with related work, and finally, Section 8 summarizes the paper and suggests some future work.

2. MEDIA ACCESS CONTROL-LAYER, WPA3, AND SOFTWARE-DEFINED NETWORKING

2.1 Media Access Control-layer overview

The IEEE 802.11 MAC data link layer is responsible for facilitating reliable communication between devices on a common network by arranging data into frames while also making sure it is transmitted correctly. It controls data flow to avoid overwhelming receivers, performs device identification using physical MAC addresses, and finds or repairs potential physical layer problems. To prevent collisions and provide seamless data transfer coordination, it also supervises how devices access the common communication channel [5].

According to the 802.11 standard, each device is uniquely recognized by a MAC address, which is a physical address. Ethernet or LAN addresses are other names for MAC addresses [2]. The Network Interface Card (NIC) includes this address as a hardware identifier. The MAC address is unique unless the user changes it manually. Usually demonstrated as six groups of hexadecimal numerals [4], it is a 48-bit value. In

terms of Organization, Unique Identifier (OUI), which the IEEE allocates to the NIC manufacturer, is made up of the first three bytes on the left side of the MAC address, as seen in Figure 2. The manufacturer designates the remaining three bytes as the Universally Administered Address (UAA) that is used to uniquely identify each NIC [6].

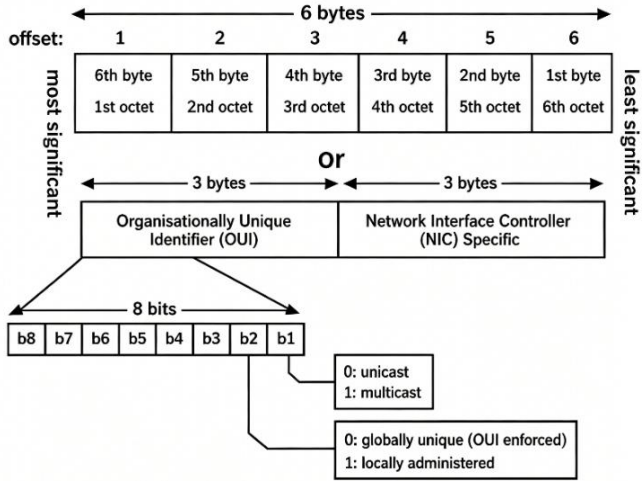

Figure 2. Structure of 48-bit Media Access Control (MAC) address [6]

MAC addresses can be categorized as unicast, multicast, or broadcast according to the least significant bit of the first octet. In practical IEEE 802.11 communication, this classification affects how frames are delivered and interpreted at the link layer, especially when management traffic is broadcast to multiple stations during discovery and coordination.

The MAC layer of IEEE 802.11 wireless networks supports three different frame types: management, control, and data frames. This defines it apart from its Ethernet cousin. While collisions cannot be detected wirelessly, it uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) instead of CSMA/CD. Important for mobility and roaming support, the MAC layer also controls device association, authentication, and handover throughout access points [7]. In comparison with data frames protected by WPA2/3 encryption, the majority of control and management frames were neither encrypted nor authenticated. This places Wi-Fi access points at considerable risk from spoofing and injection attacks [8, 9].

2.2 Wi-Fi Protected Access 3

WPA3 represents the latest Wi-Fi security standard that has been designed to replace WPA2 and to improve the protection against modern attacks. At the core of WPA3 is the SAE handshake, which replaces the WPA2 (4-way handshake) with a zero-knowledge password exchange. This mechanism allows the client and the access point (AP) to establish the shared session key with the password never being sent over the air, thus preventing attackers who may intercept the handshake and launch offline brute-force attacks on the network. WPA3 uses either 128 or 192 bits of encryption for personal networks and enterprise networks, respectively, in Figure 3, with the help of a powerful cipher, such as AES-GCM and SHA-384, to guarantee confidentiality and integrity. The most significant is that WPA3 requires Management Frame Protection (MFP), which protects against deauthentication and disassociation attacks that might have been used in the past to disconnect users. Moreover, it is forward secrecy, meaning that a different set of keys is used each time to make sure that even a subsequently compromised password will not decrypt the previous communication. WPA3 Revision 3 (2022-2023) is based on these foundations and designed to provide additional protection against side-channel attacks of the SAE handshake (as seen with Dragonblood), support downgrade protection better, and add support to IoT and resource-constrained devices with more efficient handshakes. WPA3 R3, which adds the Device Provisioning Protocol (DPP) or Easy Connect, can also be used to securely onboard devices with a QR code or NFC, enhancing usability and security in the current networks [10-13].

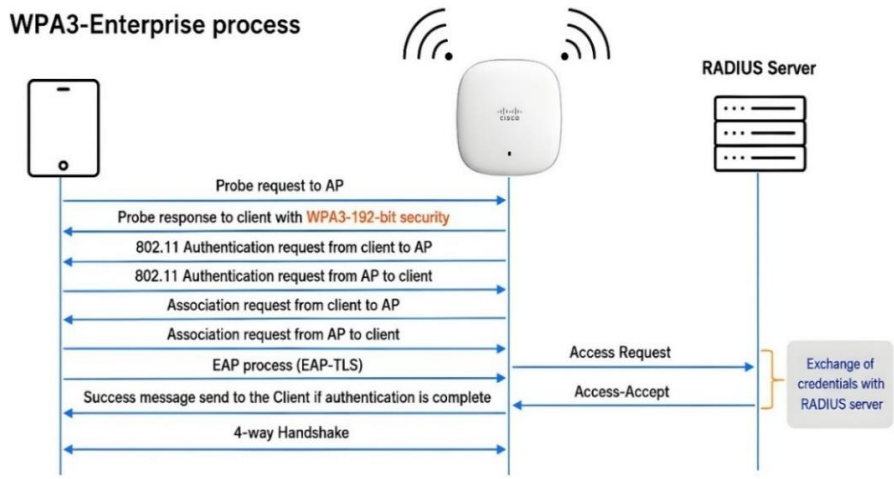

Figure 3. WPA3 enterprise process [13]

2.3 Software-Defined Networking overview

SDN is a network architecture that separates the data plane (forwarding the traffic to its destination) and the control plane (choosing how to route the data before sending it to the destination). This decoupling allows centralized control, easier programmability, and dynamic network designing with a logically centrally located SDN controller [14].

Security processes are now operating globally and not on isolated devices due to SDN's ability to offer real-time visibility to the entire network. MAC-layer attack detection and prevention in wireless networks can be performed with the

help of SDN because it is particularly effective in terms of coordinating and implementing security policies in multiple APs, Figure 4 [15]. In addition, it allows the use of southbound protocols like OpenFlow [16] for the construction of custom flow rules, traffic isolation, and anomaly response.

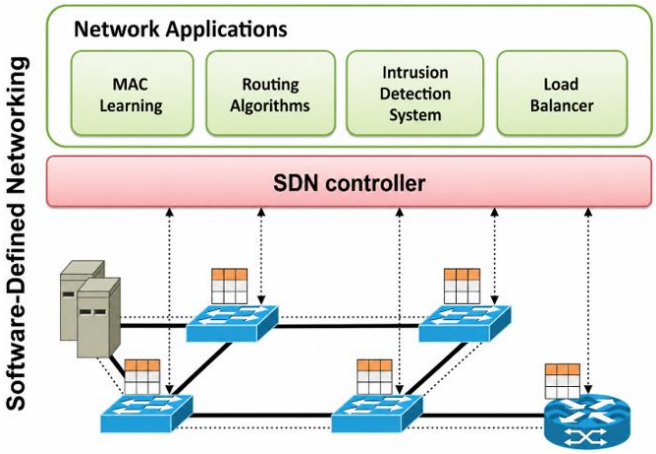

Figure 4. Software-Defined Networking (SDN) management [14]

2.4 Wireless communication and channel model

To connect the security model more directly with communications engineering, the WLAN is modeled as a wireless system in which access points and stations exchange frames over a shared channel characterized by bandwidth, transmit power, receiver sensitivity, interference, and propagation loss. Which means that the received signal strength indicator (RSSI) becomes more than a detection heuristic: it is a communication observable whose deviation from expected behavior can indicate spoofing, evil-twin activity, or abnormal mobility patterns.

At the MAC level, the same attacks can be seen as affecting contention and service. Flooding attacks increase queue pressure and channel access delay, deauthentication attacks interrupt association continuity, and rogue access points distort the relationship between SSID, BSSID, and signal characteristics. Thus, the communication degradation of an attack can be quantified by using metrics like access delay, packet delivery ratio, retransmission rate, goodput and control overhead. The communication perspective enhances the use of the proposed SDN-based framework: the controller not only supports decision-making about the presence of an attack, but also supports communication quality preservation, by early detection of abnormal PHY/MAC behavior and mitigation before it affects the whole WLAN. In subsequent sections, this view helps to support the mathematical detection model and the analysis of throughput and delay recovery.

3. RELATED WORKS

Many recent papers have discussed the security improvements of WPA3 and the remaining security issues at the MAC layer in Wi-Fi networks. These works combined provide guidance for different prevention and detection approaches. For ease of understanding and to differentiate between the strategies, we divide the literature into WPA3-based prevention, machine learning-based detection, and SDN-based security based on the methods used.

WPA3-based approaches deal with the improvement of the authentication and encryption process. Studies such as [12] and [17-22] refer to the use of critical security features like SAE, Protected Management Frames (PMF) and new cryptographic protocols that offer forward secrecy. Even with these improvements, WPA3-based solutions are still prone to practical attacks such as deauthentication, downgrade, rogue access point and side-channel attacks. Furthermore, the solutions are mainly preventive with little focus on detection and mitigation.

Machine learning approaches are based on detecting Wi-Fi attacks through data-driven learning. For instance, Saini et al. [19] present a detection system that employs machine learning to detect suspicious network traffic. These methods can identify complex attack patterns and dynamically respond to network changes. However, they often rely on training data, incur computational costs, and may not be easily explainable in real-time operation, which may hinder their use in low-latency systems.

SDN-based solutions exploit the centralised control and programmability of SDN to achieve dynamic network monitoring and control. Examples of SDN-based systems include [23-25], which show the benefits of SDN in enhancing network monitoring, traffic management and policy enforcement. But these approaches typically focus on the network layer and offer limited MAC-layer attack detection capabilities. Moreover, some SDN-based approaches address performance enhancement or quality of service (QoS) management, rather than attack mitigation, and may also introduce latency due to communication with the controller.

In general, current approaches focus on Wi-Fi security from a single angle. WPA3-based solutions prioritise prevention, machine learning-based solutions prioritise detection, and SDN-based solutions prioritise control. But these approaches are not integrated, and this limits their ability to deal with dynamic MAC-layer attacks.

4. GAP ANALYSIS

Although substantial advances have been made in Wi-Fi security, there are some problems with the current approaches from a holistic perspective. WPA3-based solutions primarily provide preventive security with improved authentication and encryption mechanisms, but do not provide real-time detection and mitigation in the event of attacks. Machine learning-based approaches enhance detection accuracy, but they come with higher computational costs, a need for training data, and a lack of interpretability, making them less attractive in scenarios that are sensitive to latency.

SDN-based solutions offer a global network view and centralised control to manage traffic and policies. However, current SDN-based approaches usually work at the higher layers of networks and do not offer fine-grained MAC-layer attack detection. Also, they typically target either generic network protection or QoS rather than Wi-Fi MAC-layer attack prevention.

As a result, there is a clear gap in the literature: the absence of a unified, lightweight, and interpretable framework that combines real-time MAC-layer attack detection with SDN-based dynamic mitigation. To fill this gap, this paper introduces a deterministic mathematical detection model with SDN control, providing explainable, timely, and MAC-layer-aware security mechanisms for Wi-Fi access points.

5. THREAT MODEL

In Wi-Fi communication, access points and central hubs are popular targets, given that any device within range of a wireless network can intercept or inject messages. Wi-Fi networks are prone to a variety of link-layer attacks that take advantage of weaknesses in the MAC layer. The fact that management and control frames (for authentication, association, deauthentication, etc.) were typically transmitted unencrypted and unauthenticated, allowing attackers to spoof them, is a common exploit used in many of these attacks [26].

MAC Address Spoofing: This attack targets the MAC address, which is the physical address of a network host or router, by changing the original address to another random or user-defined address. At the MAC layer, this allows an attacker to impersonate a legitimate device, gain unauthorized access, bypass MAC-based controls such as MAC filtering, and support other attacks such as session hijacking or eavesdropping [2].

MAC Address Flooding: The goal of these attacks is to saturate the switch's MAC address table (also known as CAM or content-addressable memory) with a large number of spoofed MAC addresses. With a full table, the switch can operate in either fail-open or fail-closed mode [10].

KRACKs: This attack exploits a weakness in WPA2-protected Wi-Fi by forcing a victim to reinstall an already used encryption key. As a result, nonce values are reset, and key material is reused, which may allow an attacker to decrypt Wi-Fi traffic and perform replay, hijacking, or content injection attacks [27].

STP Manipulation Attack: In this scenario, the attacker sends spoofed BPDUs in order to become the root bridge in the network and influence the path of traffic. Through manipulating the STP, an attacker can control traffic routing and insert itself into the communication path, allowing man-in-the-middle attacks, including eavesdropping and forged packet injection [5].

Evil Twin Rogue AP Attack: An evil twin attack occurs when a rogue access point is set up by cloning the MAC address and SSID of a legitimate AP. Victims may connect to this fake AP without noticing, allowing the attacker to intercept traffic, hijack sessions, redirect users to malicious destinations, and steal credentials [1].

Deauthentication DoS Attacks: In this attack, the attacker sends a large number of spoofed deauthentication frames to clients, causing them to be disconnected. Because 802.11 management frames may be unprotected, the attacker can falsify the source MAC address of the AP or client, continuously forcing users off the network and causing denial of service [28, 29].

6. THE SECURITY MODEL

To protect Wi-Fi networks on the MAC layer, particularly on the AP part, several conventional countermeasures have been developed to protect against such attacks as spoofing, flooding, rogue APs, and deauthentication.

MAC Address Spoofing Countermeasures: To defend against MAC address spoofing, the paper proposes 802.1X authentication so devices must authenticate with credentials rather than only MAC addresses, PMF (802.11w) to secure management frames, sequence number monitoring to detect suspicious anomalies, and RSSI analysis to identify inconsistent signal strength patterns. At the MAC layer, the strategy is to enforce identity beyond the MAC address, detect duplicate or inconsistent MAC behavior, and block spoofed management frames [30].

MAC Address Flooding Countermeasures: For MAC flooding, the proposed AP-side defenses include port security to limit how many MAC addresses can be learned on a port, rate limiting to reduce the frequency of association requests, and association limits to avoid exhausting AP resources. The MAC-layer countermeasure is to avoid AP memory or association table overflow and to identify excessive association requests with random MAC addresses [31].

KRACK Countermeasures: The paper proposes firmware patches to address vulnerabilities in WPA2 implementation, 802.11w to secure management frames and limit attack impact, and handshake monitoring to detect four-way handshake anomalies. At the MAC layer, the aim is to prevent nonce or key reuse and detect replayed handshake messages [8].

STP Manipulation Countermeasures: To protect against STP manipulation, the paper recommends BPDU Guard, which disables ports receiving BPDUs from untrusted sources and Root Guard, which prevents designated ports from becoming root ports and manipulates topology. The MAC layer approach is to prevent unauthorised BPDUs and rogue devices from manipulating Layer 2 topology [32].

Evil Twin Rogue AP Countermeasures: To mitigate Evil Twin attacks, the paper suggests the use of rogue AP detection, which prevents clients from connecting to unauthorised APs, 802.1X server certificate verification so that clients access only legitimate APs and PMF (802.11w) to prevent deauthentication attacks often used in Evil Twin attacks. The MAC-layer defense strategy is to identify unauthorized APs mimicking SSID/BSSID values and secure association with the genuine AP through mutual authentication [33, 34].

De-authentication DoS Countermeasures: For de-authentication DoS attacks, the proposed defenses are PMF (802.11w) to secure de-authentication frames, management frame rate limiting to restrict abuse, and anomaly detection systems to identify suspicious de-authentication patterns. At the MAC layer, the strategy is to authenticate deauthentication and disassociation frames, prevent forced disconnects caused by spoofing, and maintain session stability [35, 36].

6.1 The proposed system description

The MAC layer of Wi-Fi is known to have prevalent vulnerabilities, and since management and control frames are not authenticated, attackers can spoof addresses and introduce malicious frames [37]. In order to improve the robustness of Wi-Fi APs to MAC-layer attacks, a combined security structure of SDN and mathematical detection models is suggested. It is a system to identify and prevent a high number of attacks, such as MAC address spoofing, flooding, KRACKs, STP manipulation, rogue APs, and deauthentication DoS attacks, based on a deterministic equation and rule-based logic, without depending on machine learning or external behavioural training.

6.2 The proposed Mathematical detection model

6.2.1 Media Access Control address spoofing detection

RSSI variations can help detect spoofing. In the proposed scheme, spoofing is identified based on sequence number consistency and *RSSI* deviation [9]. Let S_i be the sequence

number of the i-th frame and $RSSI_i$ the signal strength. Let $RSSI_{ref}$ be the normal signal pattern of legitimate devices. $Theta_s$ is the sequence gap threshold to detect anomalous frame sequence patterns and ε_r is the *RSSI* threshold to detect inconsistent signalling.

$$Delta\ S_i = abs(S_i - S_{i-1}) \tag{1}$$

$$\Phi_{spoof(i)} = \{1, if\ Delta\ S_i < Theta_s \text{ OR } \text{abs}(RSSI_i - RSSI_{ref}) > \varepsilon_r;\ 0, \text{otherwise}\} \tag{2}$$

6.2.2 Media Access Control address flooding detection

Flooding attacks can be detected by statistically monitoring request rates [38]. In our model, MAC flooding is detected by counting the number of authentication requests during a time window. Let $N_{auth(t,T)}$ be the number of authentication requests in the time window T, $R_{auth(t)}$ be the authentication request rate, and R_{max} be the maximum acceptable authentication request rate, respectively, used to separate normal and flooding attacks.

$$R_{auth(t)} = \frac{N_{auth(t,T)}}{T} \tag{3}$$

$$\Phi_{flood(t)} = \{1, if\ R_{auth(t)} > R_{max}\ ;\ 0, otherwise\} \tag{4}$$

6.2.3 Key Reinstallation Attacks detection

KRACK attacks involve nonce reuse in the WPA2 4-way handshake [8]. KRACK is detected in the proposed model by detecting unusual repetition of handshake messages and nonce reuse in addition to normal retransmissions. Let $Nonce_i$ be the nonce value of the i-th handshake message and $Msg3_i$ be the third message in the 4-way handshake. Let $Delta\ t_i$ be the time difference between consecutive handshake events, and tau_r the time threshold to distinguish between malicious retransmissions and normal retransmissions.

$$\Phi_{krack(i)} = \{1, if\ (Nonce_i = Nonce_{i+1} \text{ AND } (Msg3_i = Msg3_{i+1} \text{ AND } (Delta\ t_i > tau_r);\ 0, otherwise\} \tag{5}$$

To prevent false positives, the KRACK detector does not use only the reuse of nonces, as repeated handshakes may also occur for normal retransmissions in poor wireless channel conditions. So, the model uses the combination of nonce reuse, repeated observation of Message 3, and the time criterion (Delta $t_i > tau_r$). This lowers the likelihood of false positives for normal retransmissions. However, false positives may still occur in highly congested channels or under severe packet loss, where repeated handshake messages appear abnormal. False negatives may occur in the case of an adversary imitating normal retransmission or in the case of observing partial traces of the handshake at the access point.

6.2.4 Spanning Tree Protocol manipulation detection

The details of STP operation have been well studied under network topology changes [39]. Under the proposed model, *STP* attacks are detected based on the presence of non-trusted Bridge Protocol Data Unit (BPDU) messages from devices trying to change the network topology. Let $BPDU_i$ be an indicator of the presence of a BPDU frame in the i-th event, and $MAC_{src(i)}$ be the source MAC address of the frame. Let *T* be the set of trusted *MAC* addresses of switches or access points.

$$\Phi_{stp(i)} = \{1, if\ BPDU_i = 1 \text{ AND } MAC_{src(i)} \notin T;\ 0, otherwise\} \tag{6}$$

6.2.5 Evil Twin Rogue access point detection

Network identity and signal anomalies can be used to detect rogue access points [40]. In the proposed model, an Evil Twin is detected by a change in the *BSSID* with the same *SSID*, and an unusual *RSSI* variance. Let $SSID_i$ be the *SSID* in the i-th frame, let $BSSID_i$ be the *BSSID* transmitting the frame, and let $RSSI_i$ be the received signal strength indicator (*RSSI*). Let $SSID_{legit}$ and $BSSID_{legit}$ be the legitimate access point *ID* and *BSSID*, and let $RSSI_{ref}$ be the reference signal profile.

$$\Phi_{evil(i)} = \{1, if\ (SSID_i = SSID_{legit}) \text{ AND } (BSSID_i \neq BSSID_{legit})\ AND\ abs(RSSI_i - RSSI_{ref}) > \varepsilon_e;\ 0, otherwise\} \tag{7}$$

6.2.6 Deauthentication denial-of-service attacks detection

Counting features can be used to detect deauthentication DoS [28]. In the considered model, deauthentication DoS is detected by observing the rate of bursts of deauthentication frames during a moving time window. Let $N_{deauth(t,T)}$ be the number of deauthentication frames in time window *T*, *D(t)* be the deauthentication frame rate, and D_{max} maximum acceptable deauthentication rate threshold.

$$D(t) = \frac{N_{deauth(t,T)}}{T} \tag{8}$$

$$\Phi_{deauth(t)} = \{1, if\ D(t) > D_{max};\ 0, otherwise\} \tag{9}$$

6.3 Key system architecture

The system operates on a centralized SDN controller that manages multiple Wi-Fi APs in a programmable network environment. As shown in Figure 5, the architecture consists of the key components.

AP Monitoring Agents: Each AP is equipped with a lightweight agent that captures 802.11 management (authentication, association, beacon, deauthentication, EAPOL frames) and control frames (ACK, RTS, and CTS) in real-time [41-43]. Feature Extraction Module: Extracts relevant MAC-layer attributes such as source/destination MAC addresses, sequence numbers, signal strength (RSSI), frame type/subtype, Timestamp, and BPDUs. These features are forwarded to the SDN controller for analysis. Mathematical Detection Engine: Implements attack-specific rule sets derived from formal models to detect anomalous behavior or protocol violations. This module evaluates real-time traffic against specific mathematical rules [44-46]. SDN Response Engine (central brain): When an attack is detected, this module issues immediate control instructions to the data plane. Mitigation includes blocking specific MAC addresses, isolating rogue APs, reconfiguring access policies, and initiating session re-keying or suppression of malicious frames.

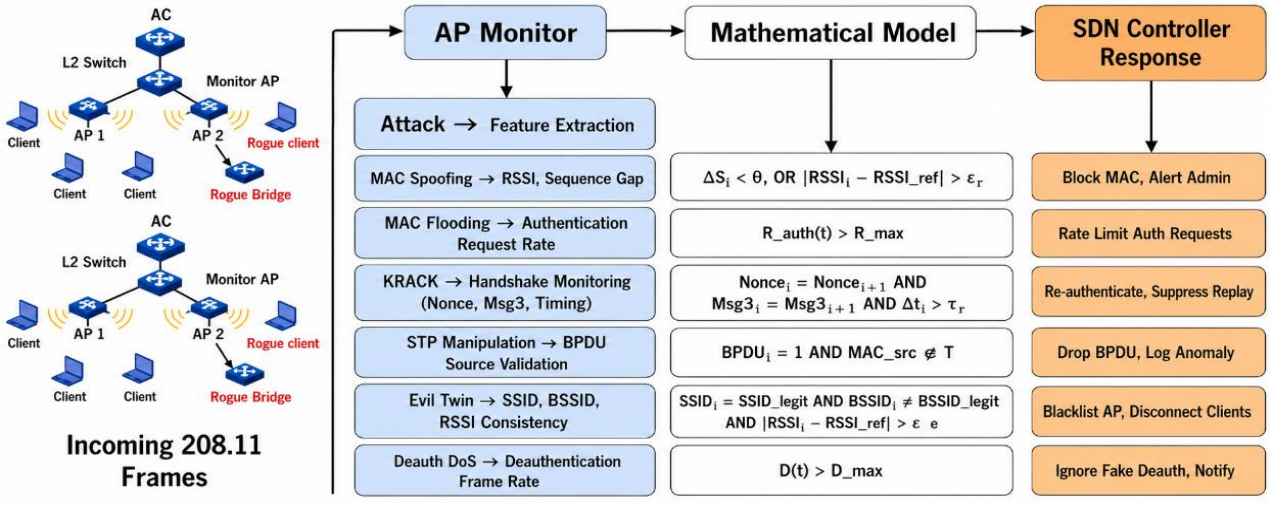

Figure 5. The system architecture

In the proposed system, AP's data plane focuses on forwarding and monitoring traffic, while the controller's control plane makes security decisions. The data flow will be from the wireless frames to the AP agent that is responsible for feature extraction, an SDN controller will use detection logic, and then the mitigation commands will make network enforcement. This enables a closed-loop security mechanism for continuous monitoring, centralized analysis, and rapid mitigation.

6.4 Unified mathematical model for Media Access Control-layer attack detection

Let $F = \{f_1, f_2, \ldots, f_N\}$ is a set of 802.11 frames observed at the AP, and each frame contains:

$$f_i = \{MAC_{src(i)}, MAC_{des(i)}, type(i), subtype(i), RSSI_i, S_i, Nonce_i, Timestamp_i\}$$

Six binary detection functions can be defined, one for each attack type: $\Phi_{spoof(i)}$, $\Phi_{flood(t)}$, $\Phi_{krack(i)}$, $\Phi_{stp(i)}$, $\Phi_{evil(i)}$, $\Phi_{deauth(t)}$.

The Unified Detection Function is defined as:

$$\Phi_{total(i,t)} = \Phi_{spoof(i)} \vee \Phi_{flood(t)} \vee \Phi_{krack(i)} \vee \Phi_{stp(i)} \vee \Phi_{evil(i)} \vee \Phi_{deauth(t)} \quad (10)$$

The Decision Function is defined as:

$$D(i,t) = \begin{matrix} 1, if\ \Phi_{total(i,t)} = 1 \\ 0, otherwise \end{matrix} \quad (11)$$

The multi-attack set is defined as:

$$A(i,t) = \{k \in \{spoof, flood, krack, stp, evil, deauth\} | \Phi_k = 1\} \quad (12)$$

The attack classification is defined as:

$$|A(i,t)| = 1 \Rightarrow Single\ Attack \quad (13)$$

$$|A(i,t)| > 1 \Rightarrow Multi - Attack\ Condition \quad (14)$$

Finally, the SDN Response Function form will be:

$$R(i,t) = Policy(A(i,t)) \quad (15)$$

Each detection function Φ_k returns a binary value, where Φ_k=1 indicates detection of the corresponding attack and Φ_k=0 indicates normal behavior.

Table 1. Access point (AP)/ Wi-Fi Attacks and security countermeasures

Attack	Detection Function
Media Access Control (MAC) Address Spoofing	$\Phi spoof\ (i) = \begin{cases} 1, if\ \Delta S_i < \theta_s OR\ \lvert RSSI_i - RSSI_{ref} \rvert > \varepsilon_r; \\ 0, otherwise \end{cases}$
MAC Address Flooding	$\Phi flood\ (t) = \begin{cases} 1, if\ R_{auth(t)} > R_{max} \\ 0, otherwise \end{cases}$
Key Reinstallation Attack (KRACK)	$\Phi krack\ (i) = \begin{cases} 1, if\ (Nonce_i = Nonce_{i+1})\ AND \\ (Msg3_i = Msg3_{i+1})\ AND\ (\Delta t_i > \tau_r); \\ 0, otherwise \end{cases}$
Spanning Tree Protocol (STP) Manipulation	$\Phi stp\ (i) = \begin{cases} 1, if\ BPDU_i = 1\ AND\ MAC_{src(i)} \notin T \\ 0, otherwise \end{cases}$
Evil Twin Rogue AP	$\Phi evil\ (i) = \begin{cases} 1, if\ (SSID_i = SSID_{legit})\ AND\ (BSSID_i \neq \\ BSSID_{legit})\ AND\ \lvert RSSI_i - RSSI_{ref} \rvert > \varepsilon_e \\ 0, otherwise \end{cases}$
Deauthentication denial of service (DoS)	$\Phi_{deauth}(t) = \begin{cases} 1, if\ D(t) > D_{max} \\ 0, otherwise \end{cases}$

The aggregate detection function is the logical OR function of all attack detection functions. The attack is detected if any of the detection functions are activated. The set A(i,t) denotes the attacks, which can be used to detect a single or multiple attack conditions. The unified detection function also offers a consistent and reproducible decision-making process, in which multiple attack conditions can be detected and simultaneously mapped to SDN attack mitigation actions via the policy at the controller. The six attack-specific detection functions are defined in Table 1.

6.5 Mapping the security system to the Transmission Control Protocol/Internet Protocol model

The proposed security system mainly operates at the data link layer (L2) level, where attacks are detected through the inspection of MAC-layer features, including sequence numbers, frame types, received signal strength indicator (RSSI), and management frame behavior. The access points communicate with the SDN controller on the network layer and transport layer (L3-L4), while the core of the detection system and the decision-making for mitigation is executed on the application layer (L5). This layered integration enables low-level MAC-layer inspection combined with centralized SDN-based control and response.

6.6 Data and control flow

Normal client traffic flows from APs to the wired network (and vice versa) as usual (data plane), with minimal interruption. To reduce overhead, the AP agent solely relays or transmits metadata to the controller, like frame headers, RSSI, and counts, instead of all user traffic. Upon detecting as saults using this metadata, the SDN controller sends commands for control back to the network. As an example, the controller might instruct the switch or AP to delete packets from a MAC spoofing attack if it is discovered. While the APs carry out light-duty monitoring and enforcement, this out-of-band control flow guarantees that complex decision-making happens centrally. Such a method ensures the efficiency of the data plane while dynamically reconfiguring the network in response to threats through using SDN's flexible control plane.

6.7 Software-Defined Networking Implementation Mechanism via OpenFlow

The proposed architecture uses SDN to enable centralized MAC-layer attack detection and mitigation [16, 47, 48]. Wireless access points capture and extract MAC-layer features from the wireless network traffic, and send the extracted features to the SDN controller [49-51]. The controller utilises the proposed mathematical detection model to detect anomalies. When an attack is detected, the controller dynamically program rules via OpenFlow to enforce mitigation actions such as banning malicious MAC addresses [52-55], restricting authentication attempts or preventing deauthentication floods. This allows real-time detection and control actions while ensuring seamless operation of the Wi-Fi network [56-58]. Table 2 shows the monitored features, detection rules, and SDN actions for different types of attacks.

Table 2. Attack features and detection conditions

Attack	Features Monitored	Mathematical Condition with (Example Thresholds)	Software-Defined Networking (SDN) Controller Response
Media Access Control (MAC) Spoofing	Sequence number patterns, MAC address reuse	$\Delta S_i < \theta_s$, θ_s = 5 sequence gaps (sudden sequence number drop from the same MAC)	Drop+log as spoofing attempt
MAC Flooding	Frame rate per MAC address	$R_{auth(t)}=N_{auth(t,T)}/T$; if $R_{auth(t)}>R_{max}$. R_{max}=30 auths/sec.	Drop or rate-limit source
Key Reinstallation Attack (KRACK)	Nonce reuse in EAPOL 4-way handshake	($Nonce_i=Nonce_{\{i+1\}}$) AND ($Msg3_i=Msg3_{\{i+1\}}$) AND ($\Delta t_i>\tau_r$)→Key reinstallation (event-based, not rate-based)	Rekey client + alert
Spanning Tree Protocol (STP) Manipulation	BPDU messages, unknown sources	$MAC_{src(i)} \notin T$ (use static trusted list)	Drop BPDU frames
Evil Twin Rogue Access Point (AP)	RSSI anomaly, SSID duplication, unverified BSSID	($SSID_i=SSID_{legit}$) AND ($BSSID_i \neq BSSID_{legit}$) AND $\lvert RSSI_i - RSSI_{ref} \rvert > \varepsilon_e$, ε_e=10 dB	Disconnect
Deauthentication Denial of Service (DoS)	Sudden spike in Deauth frames	$D(t)=N_{deauth(t,T)}/T$; if $D(t)>D_{max}$. D_{max}=10 frames/sec	Drop+block attacker MAC

6.8 Experimental setup

To test the proposed SDN-based approach for detecting attacks at the MAC layer, we created a simulation environment that models the behavior of an IEEE 802.11 wireless network under normal and attack scenarios. This environment comprises an AP, several clients, and a logically centralized control system for monitoring and decision making, as per SDN principles. It extracts MAC-layer attributes from the traffic and dynamically applies the proposed mathematical detection functions.

Data collection for traffic generation was programmed using Python scripts, where each traffic record is an abstracted Wi-Fi frame with the following attributes: MAC_{src}, MAC_{des}, frame type/subtype, $RSSI_i$, sequence number (S_i), nonce values ($Nonce_i$), and timestamp ($Timestamp_i$). We generated 1000 traffic records, including normal and attack traffic. Legitimate traffic was generated through typical communication scenarios including authentication, association and data transfer. Attacks were introduced by manipulating the following MAC-layer attributes based on attack types:

- MAC spoofing: emulated using MAC address changes and abnormal sequence number gaps and RSSI variations
- MAC flooding: emulated by raising authentication request rates
- KRACK: emulated through nonce reuse combined with abnormal retransmission timing

• STP manipulation: simulated by introducing unauthorized BPDU frames from non-trusted nodes

• Evil Twin: generated by duplicating *SSID* with mismatched *BSSID* and abnormal *RSSI* behavior

• Deauthentication DoS: generated by sending a series of deauthentication frames within a short time window

Our detection thresholds were set as:

θ_s=5 (sequence gap threshold)

ε_r=10 dB (RSSI threshold for spoofing)

R_{max}=30 requests/sec (authentication rate threshold)

τ_r=100 ms (KRACK retransmission threshold)

ε_e=10 dB (Evil Twin RSSI threshold)

D_{max}= 10 frames/sec (deauthentication threshold)

The simulation data set includes around 80% legitimate traffic and 20% attacks, with equal representation for all six attack types. The simulation environment was set up on an Ubuntu system and the SDN network was simulated using Mininet. The SDN controller, traffic generation, feature extraction and detection were integrated into this environment using Python scripts to provide a controlled environment for detection implementation and mitigation. The generated data set was also preserved and used for the performance analysis of the detection mechanism. This setup enables controlled, reproducible and repeatable testing with realistic statistical characteristics of Wi-Fi traffic and attack events.

7. SIMULATION-BASED EVALUATION, ATTACK DISTRIBUTION ANALYSIS, AND DISCUSSION

In this section, the proposed SDN-based MAC-layer security model using 1,000 simulated Wi-Fi traces was tested. The analysis focuses on whether the model can do two things at the same time: detect MAC-layer attacks with interpretable rules and preserve communication quality after mitigation. To achieve this, the data set was built with WLAN observables that are directly associated with PHY/MAC layer characteristics, such as sequence-number continuity, RSSI variance, rate of authentication requests, flags for nonce reuse, trust indicators for bridge protocol data units (BPDUs), SSID authenticity, and deauthentication bursts. These observables were selected because they capture measurable changes in channel access, management-frame behavior, signal consistency, and session continuity during attack conditions.

7.1 Attack detection criteria

The attack classes were detected using deterministic thresholds at the access point. This is one of the main contributions of the study: the detection model is explainable because every alarm is tied to a measurable abnormality in WLAN behavior rather than to a black-box classifier. In practical terms, the rules translate MAC-layer attacks into visible communication symptoms such as sequence discontinuity, abnormal signal deviation, excessive authentication pressure, handshake inconsistency, or bursty deauthentication activity.

- MAC Spoofing MAC Spoofing was detected when sequence behavior became inconsistent or when the measured RSSI profile departed from the expected transmitter pattern. This finding shows that identity misuse can be exposed through a combination of frame ordering and signal-consistency checks. Triggered when a sudden drop in sequence numbers or abnormal RSSI deviation is observed ($\Delta S_i<\theta_s$ OR $|RSSI_i-RSSI_{ref}|>\varepsilon_r$).
- MAC Flooding: Identified through excessive authentication requests per unit time ($R\_auth(t)>R\_max$). The result highlights how flooding attacks can be interpreted as communication overload events that increase contention and pressure the association process at the access point.
- KRACK: These attacks were mainly detected using nonce reuse in the 4-way WPA2 handshake. To prevent false positives in real deployment, our proposed intrusion detection model also considers re-sending of Message 3 and unexpected retransmission time as verification criteria, i.e., $(Nonce_i = Nonce_{\{i+1\}})$ AND $(Msg3_i = Msg3_{\{i+1\}})$ AND $(\Delta t_i > \tau_r)$. This verifies that handshake events can be detected in the communication phase, i.e., secure link establishment should not change.
- STP Manipulation: Inferred from receipt of BPDUs originating from untrusted sources ($MAC_{src(i)}\notin T$). Although this event is control-plane oriented, the result remains important because unstable forwarding behavior ultimately degrades traffic delivery and end-to-end communication reliability.
- Evil Twin: Recognized by SSID duplication combined with abnormal RSSI inconsistencies, i.e., ($SSID_i=SSID_{legit}$) AND ($BSSID_i\neq BSSID_{legit}$) AND $|RSSI_i-RSSI_{ref}|>\varepsilon_e$. This result emphasizes that rogue-network detection benefits from joining network identity checks with communication observables from the wireless signal environment.
- Deauth DoS: Based on excessive deauthentication frame bursts beyond threshold ($D(t)> D_{max}$) . Among the modeled events, this attack had one of the clearest communication effects because it repeatedly breaks association continuity for legitimate stations.

7.2 Statistical detection results

Most of the traffic was observed to be benign (no attack), with 808 out of 1,000 samples (80.8%) not exhibiting any malicious behavior. The remaining 192 entries were marked with specific attack types as shown in Table 3. This is an important finding because it indicates that the rule set preserves a stable baseline instead of over-labeling ordinary WLAN behavior as malicious. At the same time, the abnormal samples were still separated clearly enough to support targeted mitigation for multiple MAC-layer attack patterns.

Table 3. Statistical detection results

Proportion (%)	Count	Attack Type
80.8%	808	Benign
6.2%	62	Media Access Control (MAC) Flooding
4.6%	46	Spanning Tree Protocol (STP) Manipulation
2.5%	25	Evil Twin Rogue Access Point (AP)
2.2%	22	Key Reinstallation Attack (KRACK)
2.0%	20	MAC Spoofing
<2% total	~17	Other Combinations (Multi-Attack)

7.3 Visual and dimensional analysis

To demonstrate the unique characteristics of various attack types based on the extracted features, a Principal Component Analysis was performed. As shown in Figure 6, every point is

a traffic sample projected in a 2-dimensional space computed by Principal component analysis (PCA), showing the type of attack (or "No Attack" found).

Figure 7 summarizes the distribution of the identified attack categories in the simulated traffic. Together, Figures 6 and 7 demonstrate that the dataset has a realistic ratio of benign traffic in contrast to the observed variety of MAC-layer attack manifestations. This balance demonstrates that the framework is designed for realistic WLAN monitoring rather than for an artificially attack-heavy environment. Overall, the detection outcomes demonstrate that our mathematical model is a communication-aware security framework with interpretability. The significant outcome here is not just successful attack detection, but also the possibility to trace alarms back to communication anomalies, resulting in improved interpretability and applicability.

These experiments show that the mathematical detection algorithm is performing the function of accurately identifying legitimate and attack traffic with MAC-layer features. The ability to distinguish and separate different types of attack even in overlapping scenarios can be seen as the potential of rule-based SDN- based detection models.

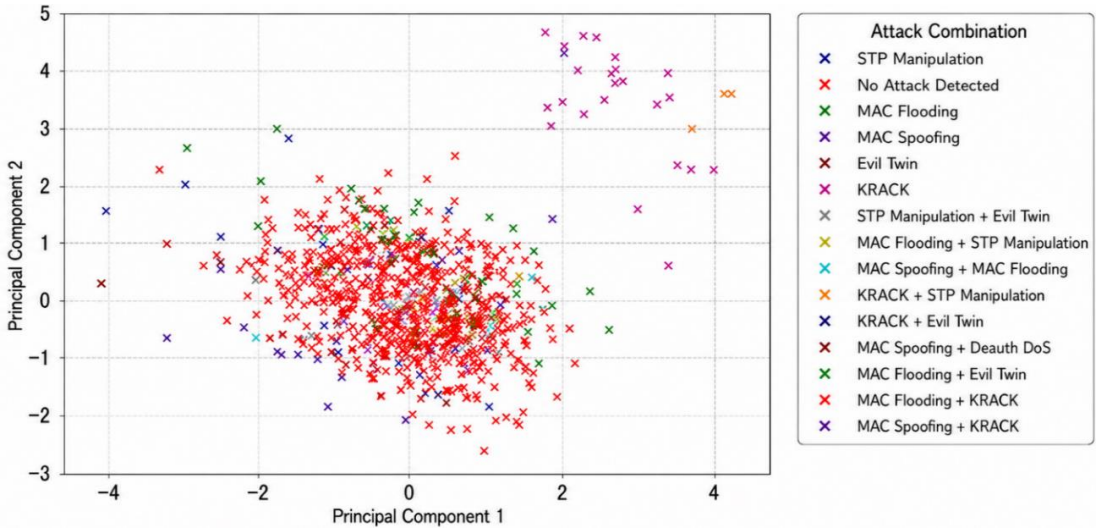

Figure 6. Principal component analysis (PCA) scatter plot of all detected attack combinations showing clustering of attack vs. benign traffic samples

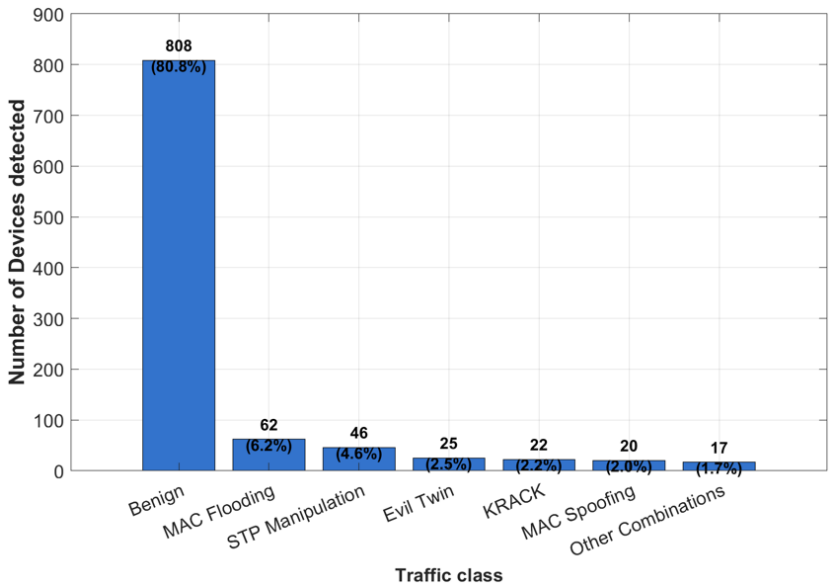

Figure 7. Distribution of benign and detected Media Access Control (MAC)-layer attack traffic in simulated WiFi traffic

7.4 Performance impact of the proposed mathematical detection model

The second contribution of the study is an assessment of the communication performance before and after mitigation. The model was tested with delay, control plane efficiency, and throughput to see whether SDN-based mitigation enables WLAN users to recover service following an attack. The findings reveal that the framework is still efficient in terms of control since the controller deals with only small metadata like MAC headers, summaries of RSSI, packet count and alarm flag instead of the whole traffic. The approach alleviates the control overhead and facilitates timely mitigation, which is critical for communication restoration in Wi-Fi.

In order to assess the communication aspects of the proposed SDN-based detection framework, the average delay and throughput are the main metrics of interest. The average end-to-end delay is given as:

$$Delay_{avg} = \left(\frac{1}{N}\right) \Sigma \left(t_{receive(i)} - t_{send(i)}\right) \quad (16)$$

where, N is the number of successfully received frames, $t_{end(i)}$ is the time frame i was sent, and $t_{receive(i)}$ is the corresponding time of arrival at the destination. The throughput is defined as:

$$Throughput = \frac{Total_{received_{data}}}{T} \quad (17)$$

Figure 8 shows that the mean delay under attack ranges from approximately 90 ms to 150 ms, depending on the attack type, with KRACK and deauthentication denial-of-service producing the largest disruption because they directly affect handshake stability and session continuity. Once the attacks are mitigated, the delay reduces to a range of around 45 to 60 ms for all the attack scenarios. This is a key contribution of the paper as it demonstrates that the SDN actions recover more stable channel access and enhance network responsiveness.

The same recovery pattern is also observed for throughput in Figure 9. When attacks occur, throughput declines significantly, reaching almost 0.5 Mbps for the most severe attack, and remains below 2.5 Mbps for the other attacks due to flooding, disconnections, and confusion in identity or routing. Throughput is restored to 5.0 to 5.4 Mbps for all attacks after mitigation. This shows the framework not only blocks the attack, but retains bandwidth and provides service continuity for legitimate users.

Although packet delivery ratio and goodput are not plotted separately, the combined reduction in delay and recovery in throughput indicates a substantial improvement in post-mitigation communication quality. Overall, the results support the paper's main claim that the proposed framework complements WPA3 by adding real-time MAC-layer attack detection, explainable decision logic, and measurable communication-performance recovery in IEEE 802.11 WLANs.

The metrics presented in Figure 8 and Figure 9 are the average values of several simulation runs, and the trends in these results show the repeatability of the performance under these conditions.

With Total_received_data being the total data successfully received (in bits), and T the duration of the observation period. The metrics are measured at the MAC layer and demonstrate the effects of the attack environment and SDN-based defense on the network communication channel, frame delivery, and network continuity.

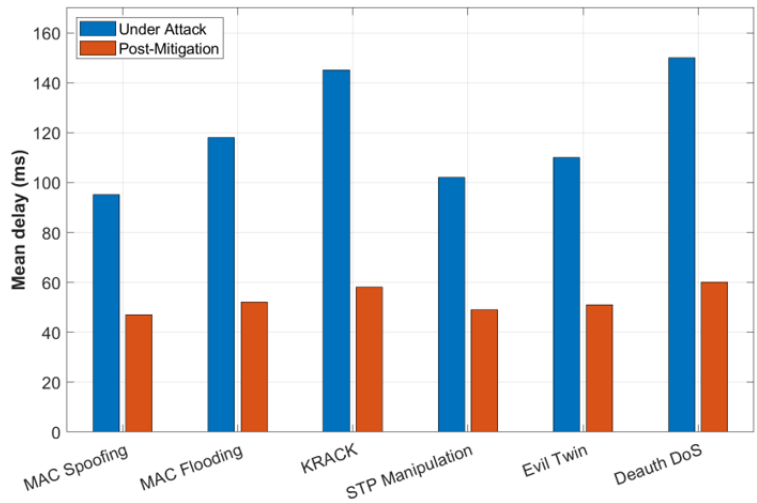

Figure 8. Delay comparison under attack and after Software-Defined Networking (SDN) mitigation

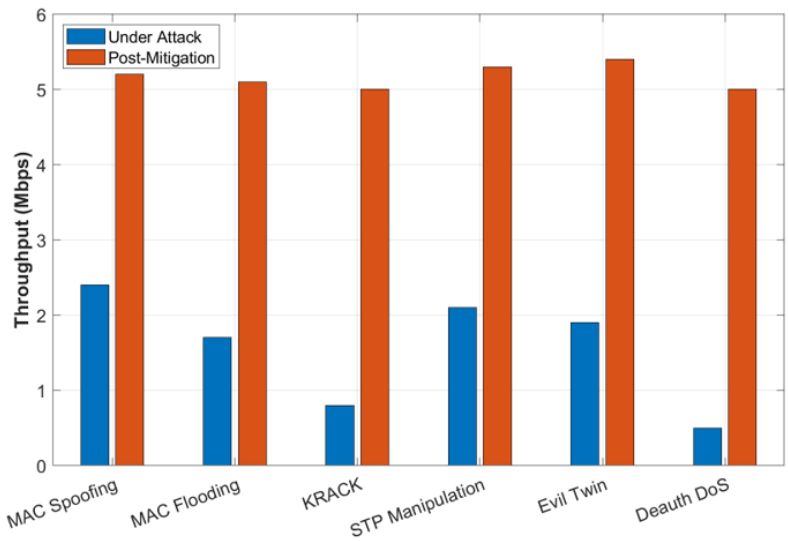

Figure 9. Throughput comparison under attack and after Software-Defined Networking (SDN) mitigation

7.5 Comparative analysis

The results in Figures 8 and 9 are compared with representative methods from the literature. In comparison to SDN-based solutions [23, 24], the proposed approach experiences similar delay (45-60 ms) but operates under wireless MAC layer constraints and explicitly measures throughput recovery from 0.5-2.5 Mbps (under active attack) to 5.0-5.4 Mbps (after attack mitigation).
Compared to WPA3-based approaches [19, 59], which introduce higher delay (130-160 ms and up to 500 ms), and do not offer quantitative throughput analysis or throughput recovery under active attack, the proposed solution exhibits lower delay and restores communication performance without the cryptographic overhead and post-detection operation. Moreover, QoS-based SDN-based approaches (e.g. [25]) prioritise traffic flows rather than preventing attacks, and provide limited throughput assurance (≈2-7 Mbps for different traffic classes) while the proposed SDN-based framework achieves similar throughput recovery regardless of the attack. The above findings prove that the proposed SDN-based, rule-driven approach represents a useful enhancement of current solutions.

7.6 Limitations and real-world deployment considerations

Although the SDN-based anomaly detection framework has proven to be effective in detecting anomalies using simulated Wi-Fi traffic, this evaluation was done in a controlled synthetic environment. Simulation provides the flexibility to inject attacks and fine-tune parameters, but it may not account for all real-world factors in wireless networks.

There are a number of potential issues that may impact detection in real-world deployments. Environmental factors such as noise, interference, multipath fading and mobility may affect RSSI and packet timing [60]. This can result in higher rates of false positives, especially for RSSI-based detection rules, such as MAC spoofing and Evil Twin detection [61, 62].

In addition, network congestion and retransmissions can be misidentified as attacks, especially for KRACK and flooding detectors that are based on repeated packets or traffic volume. This highlights the importance of adaptive threshold tuning in real deployments. Another limitation is that the current method relies on extracting features from the entire MAC frame at the access point. But partial frame capture, packet loss, or hardware limitations may affect feature extraction and detection.

Despite these challenges, the proposed approach is lightweight, explainable and can integrate with current Wi-Fi deployments. SDN allows policy adaptation, which can help to resolve some of these issues by selectively changing rules. Future work should test the proposed model in real network traces and testbeds, incorporate adaptive thresholds and environment-specific policies to ensure flexibility in dynamic wireless environments.

7.7 Practical deployment and system integration

The SDN-based MAC-layer security scheme is designed to be deployed with standard Wi-Fi deployments, with minimal hardware changes. A practical deployment can be rolled out in enterprise or campus networks, where the APs are local enforcement and monitoring points, and the SDN controller is a central detection and response point. The system can be deployed with software-based access points (e.g., hostapd) and SDN controllers (e.g., ONOS, OpenDaylight) for real-time monitoring and enforcement of traffic using OpenFlow. This framework can also be seamlessly integrated with WPA3 networks, with the proposed detection system and encryption and authentication protocols sitting together. An example use case is in corporate Wi-Fi networks with centrally administered access points and Wi-Fi devices. Here, the framework can detect and defend against MAC-layer attacks (e.g., spoofing, jamming, rogue APs) while permitting legitimate traffic. Overall, the framework provides a scalable solution to boost the security of Wi-Fi networks and close the gap between theoretical models for attack detection and real deployment.

8. DISCUSSION

The results establish the proposed model as a communication-aware protection framework for Wi-Fi access points. Its main strengths are the use of interpretable PHY/MAC observables, deterministic detection rules that map directly to known attack behaviors, and centralized SDN mitigation that restores communication stability with limited signaling overhead. The most important finding is that the framework improves both security visibility and communication quality: after mitigation, delay is reduced, throughput is recovered, and session continuity becomes more stable. This makes the model valuable not only as an intrusion-detection approach, but also as a practical method for preserving WLAN performance under MAC-layer attack conditions.

9. CONCLUSION

This paper proposes an SDN-based security architecture that incorporates mathematical detection models to protect Wi-Fi access points against a broad set of attacks at the MAC layer. Compared to current solutions, which are either threat-specific or based on non-transparent machine learning systems, the proposed system uses centralized SDN control with lightweight, rule-based logic to identify and counteract various simultaneous attacks, such as MAC spoofing, flooding, KRACK, STP manipulation, Evil Twin APs and deauthentication DoS. The system can be used to provide transparent real-time detection with low processing overhead by using deterministic equations applied to MAC-layer metadata. This is a strong way to improve the responsiveness of Wi-Fi access points and more directly deal with the shortcomings of WPA3 as a preventive protocol. The outcome is a scalable and explainable upgrade to WPA3, providing active protection and performance reliability in both new and existing Wi-Fi applications. Future research can involve adaptive thresholds, formal model verification, and commercial APs integration.

REFERENCES

[1] Agarwal, M., Biswas, S., Nandi, S. (2018). An efficient scheme to detect evil twin rogue access point attack in 802.11 Wi-Fi networks. International Journal of Wireless Information Networks, 25(2): 130-145.

https://doi.org/10.1007/s10776-018-0396-1
[2] Lalit, J. (2023). Computer network: An implementation of MAC spoofing. International Journal of Engineering and Computer Science, 12: 25717-25721.
[3] Kaur, J. (2016). Mac layer management frame denial of service attacks. In 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), Ghaziabad, India, pp. 155-160. https://doi.org/10.1109/icmete.2016.83
[4] Khasanova, A.M. (2021). Detection of attacks on Wi-Fi access points. In 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia, St. Petersburg, Moscow, Russia, pp. 28-31. https://doi.org/10.1109/ElConRus51938.2021.9396420
[5] Mahmood, S., Mohsin, S.M., Akber, S.M.A. (2020). Network security issues of data link layer: An overview. In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, pp. 1-6. https://doi.org/10.1109/iCoMET48670.2020.9073825
[6] Benzaïd, C., Boulgheraif, A., Dahmane, F.Z., Al-Nemrat, A., Zeraoulia, K. (2016). Intelligent detection of MAC spoofing attack in 802.11 network. In Proceedings of the 17th International Conference on Distributed Computing and Networking, Singapore, pp. 1-5. https://doi.org/10.1145/2833312.2850446
[7] IEEE Computer Society LAN/MAN Standards Committee. (2007). IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11. https://doi.org/10.1109/IEEESTD.2025.11184214
[8] Vanhoef, M., Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, Texas, USA, pp. 1313-1328. https://doi.org/10.1145/3133956.3134027
[9] Faria, D.B., Cheriton, D.R. (2006). Detecting identity-based attacks in wireless networks using signalprints. In Proceedings of the 5th ACM Workshop on Wireless Security, Los Angeles, California, pp. 43-52. https://doi.org/10.1145/10.1145/1161289.1161298
[10] Sagers, G. (2021). WPA3: The greatest security protocol that may never be. In 2021 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, pp. 1360-1364. https://doi.org/10.1109/CSCI54926.2021.00273
[11] Alghisi, G.A., Gringoli, F. (2024). An experimental analysis of the WPA3 protocol in IoT devices. In 2024 22nd Mediterranean Communication and Computer Networking Conference (MedComNet), Nice, France, pp. 1-4. https://doi.org/10.1109/MedComNet62012.2024.10578197
[12] Tleuberdin, S., Issainova, A., Adamova, A., Aidynov, T., Samashova, G., Satybaldina, D. (2025). Analysis of vulnerabilities and practical attacks on WPA3-enterprise in corporate wireless networks. Procedia Computer Science, 272: 613-618. https://doi.org/10.1016/j.procs.2025.10.256
[13] CISCO. WPA3 Deployment Guide. https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/wpa3-dg.html.
[14] Kreutz, D., Ramos, F.M., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S. (2014). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1): 14-76. https://doi.org/10.1109/jproc.2014.2371999
[15] Lara, A., Kolasani, A., Ramamurthy, B. (2013). Network innovation using openflow: A survey. IEEE Communications Surveys & Tutorials, 16(1): 493-512. https://doi.org/10.1109/surv.2013.081313.00105
[16] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., et al. (2008). OpenFlow: Enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2): 69-74. https://doi.org/10.1145/1355734.1355746
[17] Kohlios, C.P., Hayajneh, T. (2018). A comprehensive attack flow model and security analysis for Wi-Fi and WPA3. Electronics, 7(11): 284. https://doi.org/10.3390/electronics7110284
[18] Dalal, N., Akhtar, N., Gupta, A., Karamchandani, N., Kasbekar, G.S., Parekh, J. (2022). A wireless intrusion detection system for 802.11 WPA3 networks. In 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bangalore, India, pp. 384-392. https://doi.org/10.1109/COMSNETS53615.2022.9668542
[19] Saini, R., Halder, D., Baswade, A.M. (2022). RIDS: Real-time intrusion detection system for WPA3 enabled enterprise networks. In GLOBECOM 2022-2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, pp. 43-48. https://doi.org/10.1109/GLOBECOM48099.2022.10001501
[20] Braga, D.D.A., Kulatova, N., Sabt, M., Fouque, P.A., Bhargavan, K. (2023). From dragondoom to dragonstar: Side-channel attacks and formally verified implementation of WPA3 dragonfly handshake. In 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), Delft, Netherlands, pp. 707-723. https://doi.org/10.1109/EuroSP57164.2023.00048
[21] Halbouni, A., Ong, L.Y., Leow, M.C. (2023). Wireless security protocols WPA3: A systematic literature review. IEEE Access, 11: 112438-112450. https://doi.org/10.1109/ACCESS.2023.3322931
[22] Mykhaylova, O., Nakonechny, T. (2024). Security analysis of modern Wi-Fi network protection protocols: Assessment of WPA3 protocol resistance during attacks based on dragonblood utility. Computer Systems and Networks, 6(1): 133-147. https://doi.org/10.23939/csn2024.01.133
[23] Song, G., Hu, J., Wang, H. (2023). A novel frame switching model based on virtual MAC in SDN. International Journal of Information Security, 22(3): 723-736. https://doi.org/10.1007/s10207-022-00659-7
[24] Pradeep, S., Sharma, Y.K., Lilhore, U.K., Simaiya, S., et al. (2023). Developing an SDN security model (EnsureS) based on lightweight service path validation with batch hashing and tag verification. Scientific Reports, 13(1): 17381. https://doi.org/10.1038/s41598-023-44701-7
[25] Isolani, P.H., Kulenkamp, D.J., Marquez-Barja, J.M., Granville, L.Z., Latré, S., Syrotiuk, V.R. (2021). Delay-aware slicing and MAC management using MCDA in

IEEE 802.11 SD-RANs. In 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, pp. 331-339. https://ieeexplore.ieee.org/abstract/document/9463961.

[26] Zanna, P., Radcliffe, P., Kumar, D. (2022). Preventing attacks on wireless networks using SDN controlled OODA loops and cyber kill chains. Sensors, 22(23): 9481. https://doi.org/10.3390/s22239481

[27] Hamroun, C., Fladenmuller, A., Pariente, M., Pujolle, G. (2025). Intrusion detection in 5G and Wi-Fi networks: A survey of current methods, challenges & perspectives. IEEE Access, 13: 40950-40976. https://doi.org/10.1109/ACCESS.2025.3546338

[28] Agarwal, M., Biswas, S., Nandi, S. (2015). Detection of de-authentication dos attacks in Wi-Fi networks: A machine learning approach. In 2015 IEEE International Conference on Systems, Man, and Cybernetics, Hong Kong, China, pp. 246-251. https://doi.org/10.1109/SMC.2015.55

[29] Nguyen, T.D., Nguyen, D.H., Tran, B.N., Vu, H., Mittal, N. (2008). A lightweight solution for defending against deauthentication/disassociation attacks on 802.11 networks. In 2008 Proceedings of 17th International Conference on Computer Communications and Networks, Charlotte Amalie, United States Virgin Islands, pp. 1-6. https://doi.org/10.1109/ICCCN.2008.ECP.51

[30] Ratnayake, D.N., Kazemian, H.B., Yusuf, S.A., Abdullah, A.B. (2011). An intelligent approach to detect probe request attacks in IEEE 802.11 networks. In International Conference on Engineering Applications of Neural Networks, Corfu, Greece, pp. 372-381. https://doi.org/10.1007/978-3-642-23957-1_42

[31] Gajo, S.I. (2025). Mitigating MAC flooding attacks using port security techniques. Proceedings of the Nigerian Society of Physical Sciences, 2(1): 162-162. https://doi.org/10.61298/pnspsc.2025.2.162

[32] Cisco Systems. (2021). Chapter 13: Configuring optional spanning-tree features. In Layer 2 Switching Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches. Cisco. https://www.cisco.com/c/en/us/td/docs/switches/connectedgrid/cg-switch-sw-master/software/configuration/guide/layer2/CGS_1000_L2/l2_stpopt.html.

[33] Alotaibi, B., Elleithy, K. (2015). An empirical fingerprint framework to detect rogue access points. In 2015 Long Island Systems, Applications and Technology, Farmingdale, USA, pp. 1-7. https://doi.org/10.1109/lisat.2015.7160206

[34] Gonzales, H., Bauer, K., Lindqvist, J., McCoy, D., Sicker, D. (2010). Practical defenses for evil twin attacks in 802.11. In 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, USA, pp. 1-6. https://doi.org/10.1109/glocom.2010.5684213

[35] Schepers, D., Ranganathan, A., Vanhoef, M. (2022). On the robustness of Wi-Fi deauthentication countermeasures. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, San Antonio, USA, pp. 245-256. https://doi.org/10.1145/3507657.3528548

[36] Agarwal, M., Biswas, S., Nandi, S. (2013). Detection of De-authentication Denial of Service attack in 802.11 networks. In 2013 Annual IEEE India Conference (INDICON), Mumbai, India, pp. 1-6. https://doi.org/10.1109/INDCON.2013.6726015

[37] Alocious, C., Xiao, H., Christianson, B. (2015). Analysis of DoS attacks at MAC layer in mobile adhoc networks. In 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, pp. 811-816. https://doi.org/10.1109/IWCMC.2015.7289187

[38] Rmayti, M., Begriche, Y., Khatoun, R., Khoukhi, L., Gaiti, D. (2015). Flooding attacks detection in MANETs. In 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, pp. 1-6. https://doi.org/10.1109/SSIC.2015.7245675

[39] Indrianingsih, Y., Wintolo, H., Saputri, E.Y. (2021). Spanning tree protocol (STP) based computer network performance analysis on BPDU config attacks and take over root bridge using the linear regression method. Jurnal Online Informatika, 6(2): 155-162. https://doi.org/10.15575/join.v6i2.703

[40] Yang, C., Song, Y., Gu, G. (2012). Active user-side evil twin access point detection using statistical techniques. IEEE Transactions on Information Forensics and Security, 7(5): 1638-1651. https://doi.org/10.1109/tifs.2012.2207383

[41] Mahmood, F.E., Perrins, E.S., Liu, L. (2018). Energy consumption vs. bit rate analysis toward massive MIMO systems. In 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA. https://doi.org/10.1109/ISC2.2018.8656926

[42] Ali, Q.I. (2016). Green communication infrastructure for vehicular ad hoc network (VANET). Journal of Electrical Engineering, 16(2): 10.

[43] Ali, Q.I. (2018). GVANET project: An efficient deployment of a self-powered, reliable and secured VANET infrastructure. IET Wireless Sensor Systems, 8(6): 313-322. https://doi.org/10.1049/iet-wss.2018.5112

[44] Saeed, R.H., Ali, Q.I., Mahmood, F.E. (2026). Secure virtual reality streaming under attack: Fine-grained modeling of the latency security trade-off. International Journal of Safety and Security Engineering, 16(3): 535-545. https://doi.org/10.18280/ijsse.160307

[45] Mahmood, F.E., AlSabbagh, H.M., Edwards, R. (2012). CPW-fed UWB antenna with band-notch by hexagonal shape slot. In 2012 International Conference on Future Communication Networks, Baghdad, Iraq, pp. 69-71. https://doi.org/10.1109/ICFCN.2012.6206875

[46] Ali, Q.I. (2024). Towards more effective summative assessment in OBE: A new framework integrating direct measurements and technology. Discover Education, 3(1): 107. https://doi.org/10.1007/s44217-024-00208-5

[47] Ternon, C., Goossens, J., Dricot, J.M. (2016). FTT-openFlow, on the way towards real-time SDN. ACM SIGBED Review, 13(4): 49-54. https://doi.org/10.1145/3015037.3015045

[48] Agrawal, A., Maiti, R.R. (2025). TinyAP: A smart access point to detect KRACK on WPA2 handshake in Wi-Fi using TinyML. In 2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS), Bengaluru, India, pp. 168-173. https://doi.org/10.1109/COMSNETS63942.2025.10885765

[49] Zobary, F., Li, C. (2023). A mathematical model for sdn

control plane scalability evaluation based on controller utilization. Journal of Control Engineering and Applied Informatics, 25(4): 14-21. https://doi.org/10.61416/ceai.v25i4.8783

[50] Taima, A., Hilal, O.M., Al-Shammari, A.M., Naseriparsa, M. (2025). An empirical mathematical model to select the best controller in software-defined networks infrastructure. Al-Qadisiyah Journal for Engineering Sciences, 18(3): 233-238. https://doi.org/10.30772/qjes.2024.149238.1217

[51] Chen, J., Gopal, A., Dezfouli, B. (2021). Modeling control traffic in software-defined networks. In 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), Tokyo, Japan, pp. 258-262. https://doi.org/10.1109/netsoft51509.2021.9492632

[52] Romanov, O., Siemens, E., Nesterenko, M., Mankivskyi, V. (2021). Mathematical description of control problems in SDN networks. In Proceedings of the 9th International Conference on Applied Innovations in IT (ICAIIT), Koethen, Germany, pp. 33-39. https://doi.org/10.25673/36582

[53] Garba, U.H., Toosi, A.N., Pasha, M.F., Khan, S. (2024). SDN-based detection and mitigation of DDoS attacks on smart homes. Computer Communications, 221: 29-41. https://doi.org/10.1016/j.comcom.2024.04.001

[54] Rai, A., Barbhuiya, F.A., Sur, A., Biswas, S., Chakraborty, S., Nandi, S. (2011). Exploit detection techniques for STP using distributed IDS. In 2011 World Congress on Information and Communication Technologies, Mumbai, India, pp. 939-944. https://doi.org/10.1109/WICT.2011.6141374

[55] Murugesan, K., Thangadorai, K.K., Muralidhara, V.N. (2021). PoEx: Proof of existence for evil twin attack prevention in Wi-Fi personal networks. In 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, pp. 92-98. https://doi.org/10.1109/FiCloud49777.2021.00021

[56] Ali, Q.I., Lazim, S. (2012). Design and implementation of an embedded intrusion detection system for wireless applications. IET Information Security, 6(3): 171-182. https://doi.org/10.1049/iet-ifs.2010.0245

[57] Alsharbaty, F.S., Ali, Q.I. (2024). Smart electrical substation cybersecurity model based on WPA3 and cooperative hybrid intrusion detection system (CHIDS). Smart Grids and Sustainable Energy, 9(1): 11. https://doi.org/10.1007/s40866-024-00192-7

[58] Abdulkareem, O.A., Kontham, R.K., Mahmood, F.E. (2024). Collaborative intrusion detection system to identify joint attacks in routing protocol for low-power and lossy networks routing protocol on the Internet of Everything. Mesopotamian Journal of CyberSecurity, 4(3): 251-277. https://doi.org/10.58496/MJCS/2024/026

[59] Mathew, A., Jackson, E., Tobesman, A. (2025). Evaluating the efficacy of WPA3 against advanced attacks: A comparative analysis with WPA2 in real-world. Journal of Information Technology and Integrity, 3(1): 105. https://doi.org/10.33790/jiti1100105

[60] Abdulkareem, O.A., Kontham, R.K., Mahmood, F.E. (2024). Securing smart grids: Machine learning-driven ensemble intrusion detection for IoT RPL networks. International Journal of Safety & Security Engineering, 14(5): 1517-1525. https://doi.org/10.18280/ijsse.140519

[61] Vaidya, A., Jaiswal, S., Motghare, M. (2016). A review paper on spoofing detection methods in wireless LAN. In 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, pp. 1-5. https://doi.org/10.1109/isco.2016.7727054

[62] Banakh, R., Nyemkova, E., Justice, C., Piskozub, A., Lakh, Y. (2024). Data mining approach for Evil Twin attack identification in Wi-Fi networks. Data, 9(10): 119. https://doi.org/10.3390/data9100119