JISTecS: Journal of Information Systems, Technology and Security
ISSN 3125-1099 (online)
Vol. 1 Iss. 2 Pg. 206-225
https://ejournal.scmdigi.id/index.php/jistecs

Beyond wireless encryption: experimental assessment of DoS and spoofing vulnerabilities in campus WLANs

Azran Budi Arief*, Wardi, Samuel Panggalo, Muh. Fhadlan Dinul Haq
Universitas Hasanuddin, Makassar, Sulawesi Selatan, Indonesia
*Correspondence author: azran@unhas.ac.id
DOI: https://doi.org/10.65881/jistecs.v1i2.260

ARTICLE INFO

History:
Received: 11-10-2026
Revised: 11-15-2026
Accepted: 11-16-2026
Published: 11-25-2026

Keywords:
campus wlan security;
denial-of-service (dos);
arp spoofing;
mac-address spoofing;
cvss v4.0.

ABSTRACT

Purpose: to experimentally assess DoS and spoofing vulnerabilities in campus WLANs by evaluating their effects on network performance, communication integrity, and device identity, and determining their severity using CVSS v4.0.
Method: this study used an experimental case-study approach that integrated penetration testing and vulnerability assessment to evaluate campus WLAN security. Five attack scenarios were examined: ICMP, TCP SYN, and UDP flooding, ARP spoofing, and MAC-address spoofing. Data were collected through network performance monitoring, packet analysis, ARP-cache inspection, and MAC-address verification, with identified vulnerabilities assessed using CVSS v4.0.
Findings: ICMP, TCP SYN, and UDP flooding affected network performance and CPU utilization, while ARP spoofing produced different outcomes across the tested WLAN environments. MAC-address spoofing successfully modified the device identifier without disrupting connectivity. The vulnerability assessment reported a CVSS v4.0 score of 6.9 (Medium), highlighting the need for stronger WLAN protection beyond encryption, particularly in network availability, ARP integrity, and device authentication.
Implications: the importance of multilayered WLAN security through traffic monitoring, ARP validation, robust authentication, and access control.
Originality: lies in its integrated assessment of DoS and spoofing vulnerabilities across two campus WLAN environments using performance monitoring, packet analysis, address-mapping verification, and CVSS v4.0 scoring.

Open access article under CC–BY-SA license.

Introduction

Wireless local area networks (WLANs) have become essential infrastructure in educational institutions, supporting mobile connectivity, digital learning platforms,

institutional information systems, and academic communication services (Rawia et al., 2023). As campus activities increasingly depend on wireless connectivity, WLAN security has become critical to maintaining information confidentiality, communication integrity, and service availability (Nazir et al., 2022). However, WLAN security cannot be determined solely by implementing wireless encryption mechanisms, as it also depends on client authentication, access-point configuration, traffic isolation, and protecting communications between connected devices (Wang et al., 2025). Recent research has shown that weaknesses in wireless frame-handling mechanisms can expose network traffic or compromise connectivity even when Wi-Fi security mechanisms are in place (Schepers et al., 2023). Similarly, the SSID confusion attack shows how wireless clients can be tricked into connecting to an unintended network, highlighting the limits of relying solely on network identification and encryption (Gollier & Vanhoef, 2024). These developments reveal a fundamental security challenge: a WLAN may use standard encryption protocols yet remain vulnerable to attacks that target network availability and device identity. This situation is particularly concerning in campus environments, where disruptions to wireless services can directly affect teaching, learning, administrative operations, and access to institutional resources.

The security implications of these vulnerabilities are particularly evident in two major attack categories: denial-of-service (DoS) and spoofing attacks. DoS attacks threaten network availability by generating excessive traffic or exhausting communication and processing resources, whereas spoofing attacks undermine device identity and communication integrity by manipulating network addressing information. Previous studies have examined several dimensions of DoS and distributed denial-of-service (DDoS) attacks, including bandwidth-oriented flooding, protocol-level resource exhaustion, detection mechanisms, and mitigation strategies (Alqahtani & Abdullah, 2024; Batool et al., 2025; Su et al., 2024). ICMP, TCP SYN, and UDP flooding represent distinct traffic-generation scenarios that can produce different network conditions and performance impacts, as demonstrated by experimental datasets incorporating multiple flooding protocols and traffic intensities (Bahashwan et al., 2024). Nevertheless, increased traffic volume alone does not necessarily cause service disruption, so researchers must examine network performance and operational behaviour alongside captured packet characteristics (Hill et al., 2024). In parallel, address resolution protocol (ARP) spoofing can enable adversaries to manipulate IP-to-MAC address associations and potentially redirect communication through an attacker-controlled device. Existing research has investigated ARP spoofing detection and prevention through address-binding verification, anomaly detection, explainable deep learning, and dynamic source-address validation (Alani et al., 2023; Majumder et al., 2025; Morsy & Nashat, 2022). MAC-address spoofing introduces an additional identity-related threat by allowing a device to modify its link-layer identifier; however, such modification should be distinguished from an actual man-in-the-middle (MITM) compromise, which requires additional evidence of traffic interception or redirection. Together, these attack scenarios demonstrate the need to investigate WLAN security through measurable technical evidence rather than relying exclusively on configuration-based assessments.

Existing literature provides substantial theoretical and methodological foundations for understanding these threats, but important limitations remain in translating previous findings into practical campus WLAN security assessments. Several ARP spoofing countermeasures have been developed for software-defined networking (SDN), the Internet of things (IoT), and other specialized architectures, including controller-based detection, game-theoretic protection, and machine-learning-based

classification (Hnamte & Hussain, 2024; Jadhav et al., 2023; Mvah et al., 2024; Saritakumar et al., 2023; Usmani et al., 2022). Other investigations have explored device profiling and explainable learning techniques (Alani et al., 2023; Prasad & Chandra, 2022), as well as low-cost protection mechanisms for wireless LAN environments using Raspberry Pi devices (Nasser & Hussain, 2022). Meanwhile, research on wireless intrusion detection emphasizes the importance of appropriate feature selection and data preprocessing when identifying suspicious 802.11 traffic (Chatzoglou et al., 2022), while integrated detection frameworks highlight the value of combining indicators associated with multiple attack types (Khedr et al., 2023). Despite these contributions, much existing research focuses on individual attack mechanisms, algorithm development, or specialized network architectures. Consequently, an experimental assessment is still needed that examines multiple DoS and spoofing scenarios in a conventional campus WLAN environment and correlates attack-related packet evidence with system resource utilization, network-interface activity, ARP-cache changes, and observable communication performance. To address this gap, the present study uses an integrated experimental approach to evaluate ICMP, TCP SYN, and UDP flooding alongside ARP and MAC-address spoofing scenarios. Unlike studies that primarily emphasize attack detection or mitigation in SDN and IoT environments, this research focuses on the observable security consequences of different attack scenarios in a campus WLAN context, thereby providing a more deployment-oriented understanding of wireless network vulnerabilities.

To address the identified research gap, this study aims to experimentally assess campus WLAN vulnerabilities to selected DoS and spoofing attack scenarios by examining their effects on network availability, device identity, and communication integrity. Specifically, the assessment investigates the behavioural characteristics of ICMP, TCP SYN, and UDP flooding, evaluates ARP spoofing through changes in address mappings and traffic behaviour, and examines MAC-address spoofing as an identity-manipulation scenario. The experimental process follows a structured penetration-testing approach involving preparation, controlled attack execution, evidence collection, and post-experiment analysis, consistent with established network security assessment methodologies (Alhamed & Rahman, 2023; Kampourakis et al., 2023). The assessment also incorporates network-forensics principles to support systematic interpretation of packet-level evidence and ARP-related anomalies (Wijayanto et al., 2023). The assessment's theoretical foundation integrates the availability, integrity, and confidentiality dimensions of information security with network-layer and link-layer communication principles. The evaluation also considers measurable indicators, including packet characteristics, CPU utilization, network-interface activity, address-resolution behaviour, and communication performance. The NIST Cybersecurity Framework 2.0 provides an organizational perspective for identifying and evaluating cybersecurity risks (NIST, 2024), while the Common Vulnerability Scoring System version 4.0 (CVSS v4.0) provides a standardized framework for describing the severity of individual vulnerability findings based on exploitability and potential security impacts (First, 2024). Importantly, CVSS scores are interpreted as vulnerability-severity indicators rather than comprehensive measurements of overall organizational or network risk.

This research matters because educational institutions increasingly depend on reliable wireless infrastructure, and security incidents can disrupt network availability and undermine communication trustworthiness. A WLAN disruption can interrupt access to learning management systems, online academic resources, and administrative

services, while successful spoofing may enable unauthorized traffic redirection, interception, or manipulation. Moreover, implementing encryption does not necessarily eliminate vulnerabilities arising from network management, address resolution, or device identification. Therefore, an experimental assessment is necessary to determine whether commonly deployed campus WLAN environments provide adequate protection against these threats and to identify which attack scenarios produce the most significant observable effects. This research also offers a practical way to translate findings from specialized security studies into evidence relevant to conventional institutional wireless networks. In this context, the assessment supports a broader security perspective that combines technical observations with organizational risk considerations. The findings may subsequently inform improvements in WLAN configuration, access-control policies, network segmentation, monitoring mechanisms, and protective measures, including appropriate transport-layer encryption and policy-based access restrictions (Schepers et al., 2023). Thus, the study is important not only for identifying technical weaknesses but also for supporting informed cybersecurity decision-making and maintaining the continuity of essential campus services.

Ultimately, this research is expected to contribute to WLAN security knowledge and practice in three complementary ways. First, it provides experimental evidence concerning the effects of different DoS and spoofing scenarios on campus WLAN behavior, enabling a more systematic understanding of how distinct attack mechanisms affect network availability, device identity, and communication integrity. Second, it contributes a multidimensional assessment approach by correlating packet-level observations, network-interface activity, CPU utilization, ARP-cache behaviour, and communication performance, reducing the limitations of evaluations based on isolated indicators. Third, it provides a structured basis for interpreting experimental findings in relation to cybersecurity risk management and standardized vulnerability-severity assessment through the NIST cybersecurity Framework 2.0 and CVSS v4.0. By distinguishing traffic generation from actual service disruption, identity manipulation from verified MITM compromise, and individual vulnerability severity from overall network risk, the proposed assessment seeks to improve the accuracy and practical relevance of WLAN security evaluation. Overall, the expected contribution is an evidence-based assessment framework that can help network administrators, cybersecurity practitioners, and educational institutions identify security weaknesses, prioritize corrective actions, and strengthen the resilience of campus wireless infrastructure against evolving availability and spoofing threats.

Method

Research design and experimental approach

This study used an experimental case-study design that combined network penetration testing and vulnerability assessment to evaluate the security of a campus wireless local area network (WLAN). The assessment examined five attack scenarios: ICMP flooding, TCP SYN flooding, UDP flooding, ARP spoofing, and MAC-address spoofing. The experimental procedure consisted of three phases: (1) preparation and baseline measurement, (2) controlled attack execution and evidence collection, and (3) post-attack analysis and vulnerability severity assessment. This approach follows established penetration-testing principles involving systematic vulnerability identification, controlled testing, evidence collection, and reporting (Alhamed & Rahman, 2023). The primary unit of analysis was the victim device's network behavior

through the selected wireless access point. Each attack scenario was evaluated independently by examining network traffic, system resource utilization, address-resolution behavior, device identity, and communication performance. The findings were interpreted within the tested network environments, acknowledging that WLAN configurations and operating conditions may vary across deployments (Kampourakis et al., 2023).

Experimental environment and testing scope

The experimental environment comprised four main components: an attacker device, a victim device, a wireless access point, and a network gateway. The attacker device served as the testing endpoint, while the victim device was the primary observation target. The access point provided wireless connectivity, and the gateway served as a reference for examining address-resolution behavior and local network communication. ARP spoofing experiments were conducted separately in two wireless environments: ENG-UNHAS and Electrical LT1. Each environment was evaluated according to its documented network configuration and experimental conditions. The technical specifications of the experimental environment are summarized in Table 1.

Table 1 experimental environment and technical specifications

Component	Information to report
Attacker device	Processor, memory, operating system, and wireless-interface model
Victim device	Processor, memory, operating system, and network-interface model
Access point	Manufacturer, model, firmware, and relevant security configuration
Wireless connection	Frequency band, channel, and authentication mechanism
Software	Names and versions of traffic-generation, packet-capture, and monitoring tools

Source: primary data, processed.

The testing scope was limited to designated devices, access points, and network segments covered by the authorized assessment. Active testing required approval from the responsible network administrator, including clearly defined testing targets, schedules, traffic limitations, and termination conditions. These restrictions ensured that the experiments remained within the approved scope and followed established penetration-testing principles (Alhamed & Rahman, 2023). Relevant identifiers and sensitive communication data were also anonymized before publication, where supported by the experimental records.

Pre-attack preparation and baseline measurement

The pre-attack phase established baseline conditions by documenting the victim device's network configuration, including its IP and MAC addresses, default gateway, gateway MAC address, connected access point, and ARP-cache entries. These parameters served as references for identifying changes in device identity and IP-to-MAC address mappings during the spoofing experiments. Baseline measurements also covered network-interface activity, CPU utilization, and packet-level traffic characteristics under normal operating conditions. Captured packets were analyzed to identify protocol distribution, communication direction, and address relationships, with particular attention to gateway address consistency as an indicator relevant to ARP spoofing detection (Majumder et al., 2025; Morsy & Nashat, 2022). The baseline observation period was [insert actual duration], with measurements recorded at [insert actual sampling interval]. The resulting dataset served as a reference for evaluating network and system behavior during and after each attack scenario.

Attack scenarios and experimental evidence

Five attack scenarios were selected to assess WLAN security across three dimensions: network availability, address resolution, and link-layer device identity. Each scenario was evaluated independently using predefined objectives and evidence criteria to support consistent analysis and attribution of observed network changes. The assessment framework is summarized in Table 2.

Table 2 attack scenarios and experimental assessment criteria

Scenario	Assessment objective	Evidence examined	Interpretation boundary
ICMP flood	Examine the effect of increased ICMP traffic on network behavior	ICMP packet activity, interface traffic, CPU utilization, and observed connectivity	Increased traffic alone does not establish denial of service
TCP SYN flood	Examine the effect of increased TCP SYN traffic on communication behavior	TCP flags, traffic activity, CPU utilization, and connection behavior where recorded	SYN generation alone does not establish connection-state exhaustion
UDP flood	Examine the effect of increased UDP traffic on network performance	UDP packet activity, interface traffic, CPU utilization, and observed connectivity	Performance degradation must be distinguished from complete service interruption
ARP spoofing	Examine manipulation of local IP-to-MAC address resolution	ARP-cache changes, gateway mappings, and evidence of redirected traffic	Forged ARP packets alone do not establish MITM interception
MAC-address spoofing	Examine link-layer identity modification	MAC address before and after modification, connectivity, and relevant access behavior	Identifier modification alone does not establish MITM compromise

Source: primary data, processed.

The three flooding scenarios were selected because ICMP, TCP SYN, and UDP traffic exhibit different protocol characteristics and resource demands. Previous studies have examined their effects under varying traffic intensities and distinguished bandwidth consumption from protocol-level and computational resource exhaustion (Bahashwan et al., 2024; Batool et al., 2025; Su et al., 2024). Accordingly, packet activity, interface traffic, CPU utilization, and connectivity were used to distinguish increased traffic from actual service disruption. The ARP spoofing assessment focused on changes in the victim's IP-to-MAC address mappings, particularly those associated with the default gateway. ARP-cache records and packet-level evidence were examined to identify potential address manipulation and traffic redirection, consistent with previous research on ARP spoofing detection and prevention (Hnamte & Hussain, 2024; Jadhav et al., 2023; Majumder et al., 2025). The MAC-address spoofing assessment examined changes in the attacker's link-layer identifier and their associated connectivity and access behavior. However, successful MAC-address modification was distinguished from verified device impersonation or man-in-the-middle (MITM) interception, which requires additional evidence of unauthorized access, communication redirection, or actual traffic interception (Schepers et al., 2023).

Data collection and performance indicators

Experimental data were collected from network-monitoring records, packet captures, system-resource measurements, ARP-cache entries, MAC-address records, and connectivity observations. These sources were used to evaluate WLAN behavior under

baseline, attack, and available recovery conditions. The assessment focused on network-interface activity, CPU utilization, and communication availability. Interface traffic was examined through transmitted and received data, while CPU utilization indicated system resource consumption. Traffic measurements were interpreted according to the monitoring tool's capabilities, as total interface activity may include attack-generated packets rather than legitimate application throughput. Packet-level analysis examined protocol distribution, packet direction, TCP flags, ARP messages, and IP-to-MAC address relationships to identify flooding patterns and address-resolution anomalies. These indicators were selected based on feature-selection and data-preprocessing principles in wireless intrusion detection (Chatzoglou et al., 2022). Where available, timestamped records were used to correlate attack activity with observed performance changes. Analysis was limited to the preserved experimental evidence; screenshots and descriptive outputs were interpreted qualitatively, while statistical measures were not calculated without sufficient underlying numerical data and repeated observations.

Post-attack analysis and evidence validation

The post-attack phase compared baseline, attack-period, and available recovery observations to identify changes in WLAN behavior. For flooding scenarios, network-interface traffic, CPU utilization, packet activity, and communication performance were monitored to distinguish increased traffic and resource consumption from actual degradation or interruption of legitimate services. For ARP spoofing, validation focused on address-mapping changes and evidence of packet redirection. Modified ARP entries and unusual ARP messages were treated as indicators of potential address manipulation, while successful traffic interception required additional evidence of communication redirection through the attacker-controlled device. This approach reflects previous research on device profiling, wireless LAN protection, and ARP spoofing detection (Nasser & Hussain, 2022; Prasad & Chandra, 2022; Saritakumar et al., 2023; Usmani et al., 2022). All findings were interpreted by correlating multiple evidence sources, consistent with integrated network-attack detection and network-forensics approaches (Khedr et al., 2023; Wijayanto et al., 2023). Similarly, connection loss was treated as an observed connectivity event and attributed to an active security response only when supported by access-point, controller, or security-system logs. This approach ensured that security conclusions remained consistent with the available experimental evidence.

Vulnerability severity assessment

The severity of identified vulnerabilities was assessed using the Common Vulnerability Scoring System version 4.0 (CVSS v4.0). Scoring was applied to specific, evidence-supported vulnerability findings rather than automatically assigning scores to each attack scenario. Each finding was evaluated based on its exploitation conditions and potential confidentiality, integrity, and availability impacts, following the CVSS v4.0 specification (First, 2024). The assessment documented the affected component, demonstrated weakness, supporting evidence, selected Base metric values, metric justifications, complete CVSS vector string, numerical score, and severity rating. The evaluated metrics included Attack Vector (AV), Attack Complexity (AC), Attack Requirements (AT), Privileges Required (PR), User Interaction (UI), and the confidentiality, integrity, and availability impacts on vulnerable and subsequent systems. Metric selection reflected the actual experimental conditions. In particular, the Attack Vector was determined according to the applicable CVSS definitions, distinguishing Network from Adjacent access where appropriate. Impacts on

subsequent systems were included only when supported by evidence of effects beyond the vulnerable system. All metric selections and justifications were documented to ensure transparency and reproducibility (First, 2024). The resulting scores represented individual vulnerability severity rather than the overall security risk of the campus WLAN. Accordingly, CVSS findings were interpreted alongside the organizational risk-management perspective of the NIST Cybersecurity Framework 2.0 (First, 2024; NIST, 2024).

Methodological limitations

This study was limited to the selected access points, devices, network configurations, and observation periods. Therefore, the findings reflect the tested WLAN environments and cannot be generalized to all institutional wireless networks, as experimental conditions and attack characteristics may influence security assessment outcomes (Hill et al., 2024; Kampourakis et al., 2023). The interpretation of findings was also constrained by the availability of experimental evidence. Where attack duration, packet-generation rates, repeated trials, or timestamped measurements were unavailable, comparisons were limited to descriptive analysis. Furthermore, MAC-address modification was interpreted as identity manipulation, while increased CPU utilization and interface traffic were treated as indicators of resource loading rather than confirmed security impacts. These limitations ensured that the conclusions remained consistent with the evidence and scope of the experimental design.

Results and discussion

Pre-attack network conditions

Before executing the five attack scenarios, baseline measurements were collected to characterize the victim device's network performance and system resource utilization under normal WLAN conditions. The assessment focused on two indicators: Wi-Fi throughput and CPU utilization, which served as references for evaluating subsequent changes during the experiments. As shown in Figure 2, the throughput measurement represents the victim device's initial data-transfer performance before attack-related traffic was introduced. This measurement provided a reference for comparing network performance during the ICMP, TCP SYN, and UDP flooding experiments.



Figure 2 wi-fi throughput performance on the victim device
Source: primary data, processed.

CPU utilization was also monitored to establish the device's baseline processing workload. As shown in Figure 3, CPU utilization was about 5%, indicating relatively low processor activity under normal network conditions.

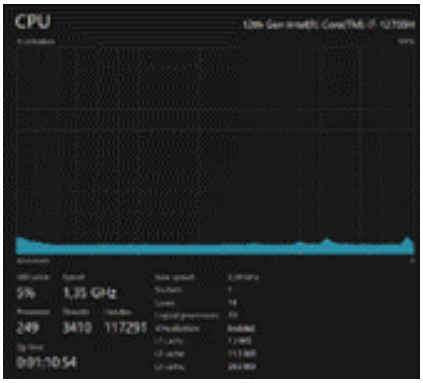

Figure 3 CPU utilization performance on the victim device
Source: primary data, processed.

Baseline observations indicate that the victim device operated under relatively normal network and system conditions, with CPU utilization at about 5% and a stable throughput baseline. These measurements provided the basis for identifying subsequent changes in network performance and resource consumption. However, the results represent only the conditions observed during the experimental period and should not be generalized to other WLAN environments.

ARP spoofing

Before the ARP spoofing experiments, the victim device's ARP cache was examined to establish baseline IP-to-MAC address mappings, particularly those associated with the default gateway. These records served as references for identifying potential address manipulation during subsequent experiments. The assessment was conducted in two wireless environments: ENG-UNHAS (WiFi 1) on the third floor and Electrical LT1 (WiFi 2) on the first floor. Each environment was examined independently to account for differences in network configuration. Figure 4 presents the victim's initial ARP cache on WiFi 1, showing the IP-to-MAC address associations before the attack.

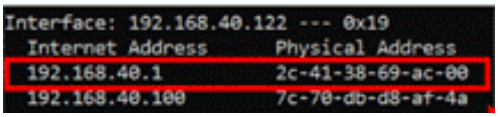

Figure 4 ARP cache before the ARP spoofing attack on WiFi 1 (ENG-UNHAS)
Source: primary data, processed.

Similarly, Figure 5 shows the initial ARP cache on WiFi 2 (Electrical LT1), providing a separate reference for evaluating subsequent changes in address resolution.

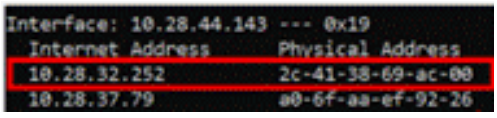

Figure 5 ARP cache before the ARP spoofing attack on WiFi 2 (Electrical LT1)
Source: primary data, processed.

These baseline records provided the basis for comparing address-resolution behavior across both environments. Since ARP spoofing can cause a victim to associate a legitimate IP address with an unintended MAC address, subsequent analysis focused on changes in gateway mappings and supporting packet-level evidence. However, ARP-

cache entries alone cannot confirm traffic interception; therefore, packet-flow observations and communication behavior were also considered when evaluating potential traffic redirection.

MAC-Address Spoofing

Before the MAC-address spoofing experiment, the attacker's network interface was inspected using the ifconfig command to identify its original media access control (MAC) address. This address served as the baseline for evaluating subsequent link-layer identity modifications. Figure 6 presents the original MAC address recorded before the experiment, providing a reference for comparison with the post-attack configuration.



Figure 6 original MAC address of the attacker's device before MAC-address spoofing
Source: primary data, processed.

The initial MAC address was subsequently compared with the modified address to determine whether the network interface's identifier had changed. However, successful MAC-address modification demonstrates only link-layer identifier manipulation and does not independently confirm device impersonation, unauthorized network access, or man-in-the-middle (MITM) interception. Such conclusions require additional evidence from connectivity observations, access-point records, and communication-redirection analysis.

Denial-of-service attack

The DoS assessment examined the effects of ICMP flooding, TCP SYN flooding, and UDP flooding on campus WLAN performance and victim-device resource utilization. The evaluation focused on Wi-Fi throughput and CPU utilization to identify changes in network activity and processing workload during each attack scenario. The three scenarios were analyzed independently to characterize their respective effects and compare their observable performance patterns. The ICMP flood experiment increased ICMP traffic and caused variations in Wi-Fi throughput, as shown in Figure 7. These changes indicate additional network-interface activity compared with the baseline condition. CPU utilization was also monitored to examine the associated processing workload. Figure 8 presents the CPU observations during the experiment, providing a basis for comparison with the baseline utilization of approximately 5%.

Figures 7 and 8 together illustrate the network- and system-level responses to increased ICMP traffic. However, changes in throughput and CPU utilization alone do not confirm successful DoS; they require evidence of degraded or interrupted legitimate communication. The TCP SYN flood experiment examined the effects of increased TCP connection-establishment traffic on network performance and processing workload. Figure 9 presents the Wi-Fi throughput observations, while Figure 10 shows the corresponding CPU utilization during the experiment. These indicators were used to examine changes in network activity and potential processing demands associated with TCP SYN traffic.

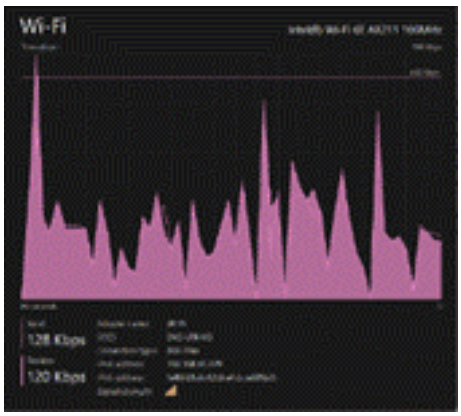

Figure 7 Wi-Fi throughput performance of the victim device during the ICMP flood attack
Source: primary data, processed.

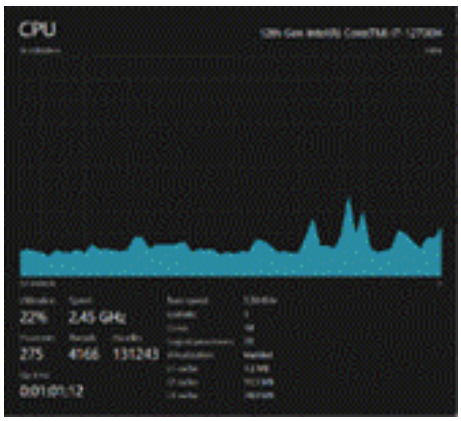

Figure 8 CPU utilization performance of the victim device during the ICMP flood attack
Source: primary data, processed.

Figures 9 and 10 provide complementary evidence of the victim device's response to TCP SYN traffic. Nevertheless, confirming service disruption requires additional evidence of impaired legitimate connection establishment or exhaustion of connection-handling resources. Therefore, the observed performance changes were interpreted as indicators of network and system activity rather than definitive evidence of successful DoS.



Figure 9 Wi-Fi throughput performance of the victim device during the TCP SYN flood attack
Source: primary data, processed.

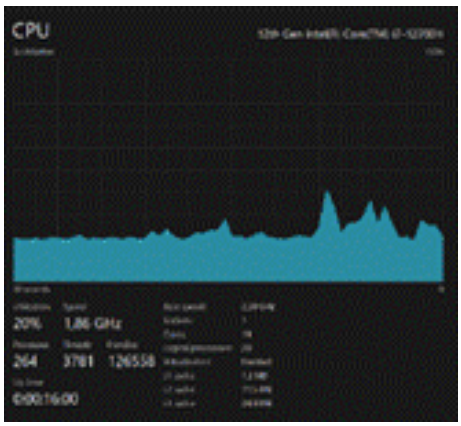

Figure 10 CPU utilization performance of the victim device during the TCP SYN flood attack
Source: primary data, processed.

Similarly, the UDP flood experiment examined how increased UDP traffic affected Wi-Fi throughput and CPU utilization. Figure 11 presents the throughput observations, while Figure 12 illustrates the corresponding CPU utilization. Together, these measurements provide an overview of network-interface activity and processing workload during the UDP flood scenario.



Figure 11 Wi-Fi throughput performance of the victim device during the UDP flood attack
Source: primary data, processed.

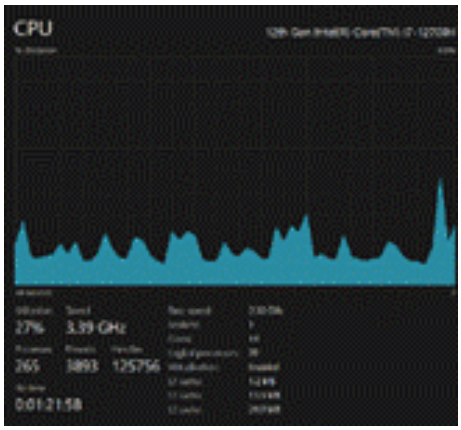

Figure 12 CPU utilization performance of the victim device during the UDP flood attack.
Source: primary data, processed.

Figures 11 and 12 show the importance of examining network performance and system resource utilization together when evaluating UDP flooding. However, increased

packet activity or CPU utilization alone does not establish service unavailability; additional evidence of degraded or interrupted legitimate communication is required. Comparing the three flooding scenarios highlights their different protocol characteristics and potential effects on WLAN performance. ICMP flooding generates ICMP traffic, TCP SYN flooding involves connection-establishment requests, and UDP flooding introduces additional UDP traffic. These differences may produce varying patterns of network activity and processing demands. Throughput and CPU utilization therefore serve as complementary indicators, as changes in traffic activity do not necessarily correspond to proportional changes in processing workload.

ARP spoofing attack

The ARP spoofing experiments revealed different responses across the two wireless environments. On WiFi 1 (ENG-UNHAS), the victim's ARP cache showed no visible changes following the attack, as presented in Figure 13. The gateway and other IP-to-MAC address mappings remained consistent with the baseline observations, indicating that no modification was detected in the victim's ARP table during the observation period.

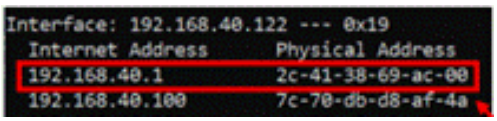

Figure 13 victim's ARP cache after the arp spoofing attack on WiFi 1 (ENG-UNHAS).
Source: primary data, processed.

Despite the unchanged ARP cache, packet analysis in wireshark on the attacker device revealed duplicate ARP packets. Furthermore, ICMP packets originating from the victim during a ping test to Google were observed on the attacker device. These findings indicate the presence of attack-related ARP traffic and suggest possible involvement of the attacker in the victim's communication. However, confirming successful man-in-the-middle (MITM) interception requires additional evidence of bidirectional traffic redirection. A different result was observed on WiFi 2 (Electrical LT1), where the victim's ARP cache displayed a modification in the gateway's MAC address, as shown in Figure 14. The recorded address changed from 2C-41-38-69-AC-00 under baseline conditions to 30-DE-4B-51-EE-ED after the attack. This change provides direct evidence of IP-to-MAC address mapping manipulation during the experiment.

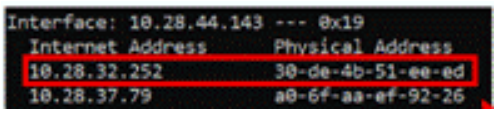

Figure 14 victim's ARP cache after the arp spoofing attack on WiFi 2 (Electrical LT1).
Source: Primary data, processed.

Additionally, the attacker's wireless connection became disconnected shortly after the attack. Although this event may indicate a response from the wireless infrastructure or an associated security mechanism, its cause cannot be confirmed without supporting access-point logs, controller records, or security alerts. Therefore, the disconnection is treated as an observed connectivity event rather than definitive evidence of automated attack detection. The experiments demonstrated different ARP spoofing responses across the two environments. WiFi 1 exhibited duplicated ARP

packets and victim-related ICMP traffic without visible ARP-cache modification, whereas WiFi 2 showed a direct change in the gateway's MAC address. These findings highlight the importance of combining ARP-cache inspection and packet-level analysis when evaluating address-resolution manipulation. Nevertheless, ARP-cache modification and attack-related packet observations alone are insufficient to establish successful MITM interception without further evidence of actual traffic redirection.

MAC-address spoofing attack

The MAC address spoofing experiment demonstrated that the attacker's network interface successfully adopted a different media access control (MAC) address from its original identifier. The network-interface configuration, shown in Figure 15, verified the change. This result confirms that the attacker's link-layer identifier was successfully changed under the tested WLAN conditions.

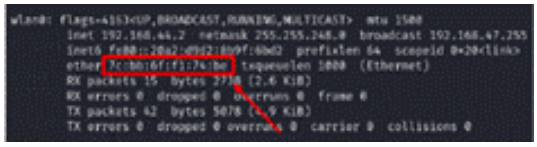

Figure 15 new MAC address of the attacker's device after MAC-address spoofing
Source: primary data, processed.

A comparison between the original and modified MAC addresses is presented in Figure 16. The results confirm a change in the identifier reported by the attacker's network interface, providing further evidence of successful MAC address modification.

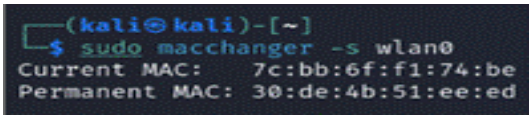

Figure 16 comparison between the original and modified MAC addresses
Source: primary data, processed.

During the observation period, the attacker's device maintained internet connectivity and communication with the victim device. This indicates that MAC-address modification did not immediately disrupt network communication. However, these observations do not, on their own, demonstrate successful device impersonation, unauthorized access, or man-in-the-middle (MITM) interception. Such conclusions require additional evidence showing that the modified address was accepted as another device's identity or enabled unauthorized network access. The security implications of the experimental findings were considered using the Common Vulnerability Scoring System version 4.0 (CVSS v4.0). The framework provides a standardized approach to evaluating vulnerability severity based on exploitation conditions and potential impacts on confidentiality, integrity, and availability (First, 2024). The selected Base metrics are presented in Table 3.

Table 3 vulnerability assessment scoring based on CVSS v4.0

Assessment metric	Scoring
Attack vector (AV)	Network (N)
Attack complexity (AC)	Low (L)
Attack requirements (AT)	None (N)
Privileges required (PR)	None (N)
User interaction (UI)	None (N)

Assessment metric	Scoring
Vulnerable system confidentiality (VC)	None (N)
Vulnerable system integrity (VI)	None (N)
Vulnerable system availability (VA)	Low (L)
Subsequent system confidentiality (SC)	Negligible (N)
Subsequent system integrity (SI)	None (N)
Subsequent system availability (SA)	Low (L)

Source: primary data, processed.

The selected metrics were used to calculate the CVSS v4.0 score. Based on the reported calculation, the assessment produced a score of 6.9, corresponding to the Medium severity category, as presented in Table 4.

Table 4 vulnerability assessment rating results

Assessment parameter	Result
CVSS v4.0 Score	6.9
Severity rating	Medium

Source: primary data, processed.

The reported Medium classification indicates a security concern that may require mitigation, particularly where network access controls rely heavily on MAC-address identification. However, the score must reflect a clearly demonstrated vulnerability, not MAC-address modification alone. The selected metrics and resulting score should also be verified against the actual exploitation conditions and complete CVSS v4.0 vector. The experiment confirms that MAC-address modification was technically feasible while maintaining network connectivity. Nevertheless, the findings do not establish successful device impersonation or unauthorized access. From a security perspective, campus WLAN deployments should avoid relying exclusively on MAC-address filtering and incorporate stronger device authentication, access-control mechanisms, and monitoring of unexpected identity changes.

Discussion

The experimental findings show that campus wireless local area network (WLAN) security cannot be evaluated solely by wireless encryption, as vulnerabilities can also arise from traffic handling, address resolution, device identification, and network access control. The ICMP flood, TCP SYN flood, and UDP flood experiments revealed changes in network throughput and CPU utilization, indicating that different flooding scenarios can impose additional traffic and processing demands on the victim device. These findings align with previous studies by Bahashwan et al. (2024); Su et al. (2024); and Batool et al. (2025), which emphasize that protocol-specific flooding attacks can produce distinct traffic characteristics and resource-consumption patterns. Nevertheless, the present findings also highlight the importance of distinguishing increased network activity from actual service disruption. Unlike studies that evaluate DDoS attacks through extensive datasets and detection frameworks, this research examines the observable performance responses of a conventional campus WLAN under controlled experimental conditions. Consequently, although all three scenarios demonstrated potential effects on network performance, the available observations do not establish that one attack was consistently more severe than the others. This finding reinforces the importance of evaluating network availability through multiple indicators, including throughput, CPU utilization, and the continuity of legitimate communication.

The ARP spoofing experiments revealed differences in responses between the two campus wireless environments: ENG-UNHAS (WiFi 1) and Electrical LT1 (WiFi 2). On WiFi 1, the victim's ARP cache showed no visible changes, although Wireshark analysis revealed duplicate ARP packets and ICMP traffic associated with the victim's communication on the attacker device. In contrast, WiFi 2 directly modified the gateway's MAC address in the victim's ARP cache, changing it from 2C-41-38-69-AC-00 to 30-DE-4B-51-EE-ED. These findings align with research by Morsy & Nashat (2022) and Majumder et al. (2025), who emphasise the importance of verifying IP-to-MAC address relationships to identify ARP spoofing. Similarly, Hnamte & Hussain (2024) and Jadhav et al. (2023) show that ARP spoofing detection and mitigation require mechanisms that can identify abnormal address mappings and communication behaviour. The differences between WiFi 1 and WiFi 2 further indicate that ARP spoofing cannot be evaluated solely through ARP cache inspection. Packet-level monitoring is also necessary because suspicious communication activity may occur without immediately producing a visible change in the victim's ARP table. Furthermore, the disconnection observed on the attacker device in WiFi 2 suggests the attack was interrupted by a connectivity-related event. However, additional access-point or security-system logs would be needed to determine whether this resulted from an automated security response.

The MAC-address spoofing experiment further demonstrated that the attacker's original MAC address could be successfully modified while maintaining internet connectivity and communication with the victim device. This finding illustrates the limitations of relying exclusively on MAC addresses for device identification in WLAN access-control policies. The result is particularly relevant to Schepers et al. (2023), whose research, Framing Frames: Bypassing Wi-Fi Encryption by Manipulating Transmit Queues, demonstrates that weaknesses in wireless frame handling and client identification can have security implications beyond conventional encryption mechanisms. Their research shows how manipulating wireless communication and access-point frame handling may enable traffic exposure, client impersonation, and denial-of-service conditions under specific vulnerable configurations. The present study complements this perspective by experimentally examining MAC-address modification in two campus WLAN environments. However, an important distinction must be maintained: the successful modification of the attacker's MAC address establishes link-layer identity manipulation, but does not independently demonstrate successful impersonation of an authorized client, unauthorized access to protected resources, or MITM interception. Therefore, the findings emphasize the importance of implementing authentication and access-control mechanisms that verify device identity beyond the MAC address. This approach also aligns with the broader security recommendations discussed by Schepers et al. (2023), particularly the use of policy-based access restrictions and transport-layer encryption to reduce the impact of wireless identity and traffic-manipulation attacks.

The combined findings from the DoS, ARP spoofing, and MAC-address spoofing experiments demonstrate that campus WLAN security involves several interconnected dimensions, particularly availability, communication integrity, and device identity verification. This observation supports the defence-in-depth perspective emphasised in the NIST Cybersecurity Framework 2.0 (NIST, 2024), which promotes systematic identification, assessment, and prioritisation of cybersecurity risks rather than dependence on a single protective mechanism. Furthermore, the results align with the methodological perspectives of Chatzoglou et al. (2022) and Khedr et al. (2023), who

emphasise the value of combining multiple traffic characteristics and security indicators when examining network attacks. In this study, throughput and CPU utilisation showed performance-related changes, ARP-cache inspection identified address-mapping modifications, and packet analysis provided additional information about communication behaviour. Together, these observations offer a broader assessment than examining individual attack indicators separately. From an operational perspective, campus network administrators should strengthen traffic monitoring, implement appropriate ARP validation mechanisms, enforce robust device authentication, and apply network segmentation and access-control policies. Transport-layer encryption should also be maintained to protect application data even when weaknesses occur at lower communication layers. These measures are particularly important in educational environments where WLAN availability and communication security directly support learning activities, academic administration, and institutional information services.

Finally, the CVSS v4.0 assessment provides a structured approach to characterising the vulnerability's severity, with the reported score of 6.9 corresponding to the Medium severity category. This assessment follows the framework established by First Inc. (2024), which evaluates vulnerability characteristics through exploitability conditions and potential impacts on confidentiality, integrity, and availability. However, the CVSS score should be interpreted in relation to the specific vulnerability and its documented exploitation conditions rather than as a comprehensive measurement of the entire campus WLAN security level. In particular, successful MAC address modification should not automatically be treated as an independently scored vulnerability without establishing the underlying weakness in authentication or access-control enforcement. This research therefore experimentally examines multiple WLAN attack scenarios in real campus wireless environments and integrates performance monitoring, ARP-cache inspection, packet-level analysis, and vulnerability severity assessment. Unlike studies that focus on individual attack-detection algorithms, SDN-based environments, or laboratory datasets, this study offers a comparative view of the observable security behaviour of two campus WLAN access-point environments. The findings contribute to a more comprehensive understanding of why wireless encryption alone cannot guarantee WLAN security and provide empirical guidance for developing more resilient campus network protection strategies.

Conclusions

This study evaluated campus wireless local area network (WLAN) security through five experimental scenarios: ICMP flooding, TCP SYN flooding, UDP flooding, ARP spoofing, and MAC-address spoofing. The flooding experiments revealed changes in network throughput and CPU utilization, indicating additional network traffic and processing demands. However, the available evidence was insufficient to establish definitive service disruption or compare attack severity. The ARP spoofing experiments demonstrated different responses across the two wireless environments: ENG-UNHAS showed attack-related ARP and ICMP traffic without visible ARP-cache changes, whereas Electrical LT1 exhibited a modification of the gateway's MAC address. Meanwhile, the MAC-address spoofing experiment confirmed successful identifier modification while maintaining network connectivity. The reported CVSS v4.0 assessment produced a score of 6.9 (Medium), subject to validation of the selected metrics and the specific vulnerability assessed. Overall, the findings demonstrate the importance of evaluating WLAN security beyond encryption by considering network availability, address-resolution integrity, and device-identity verification.

From a practical perspective, this study provides an integrated experimental assessment combining network performance monitoring, packet analysis, ARP-cache inspection, MAC-address verification, and vulnerability assessment. The findings highlight the importance of strengthening campus WLAN security through ARP validation, reliable device authentication, access-control enforcement, network monitoring, and transport-layer encryption. However, the results are limited to the tested devices, access points, network configurations, and observation periods. The absence of comprehensive quantitative measurements, complete security logs, and sufficient evidence of successful MITM interception also restricts the scope of the conclusions.

Future research should extend testing to additional access points, devices, and network environments, supported by repeated experiments under standardized conditions. Quantitative evaluation using throughput, packet loss, latency, CPU utilization, and service availability would enable more reliable comparisons of attack impacts. Further investigations should also incorporate packet-flow analysis and access-point security logs to verify traffic interception, device impersonation, and automated security responses. Finally, evaluate the effectiveness of mitigation mechanisms, including Dynamic ARP Inspection, IP-MAC binding, network segmentation, stronger authentication, and intrusion detection systems, to support the development of more resilient campus WLAN infrastructures.

References

Alani, M. M., Awad, A. I., & Barka, E. (2023). ARP-PROBE: An ARP spoofing detector for Internet of Things networks using explainable deep learning. *Internet of Things*, *23*, 100861. https://doi.org/10.1016/j.iot.2023.100861

Alhamed, M., & Rahman, M. M. H. (2023). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences*, *13*(12), 6986. https://doi.org/10.3390/app13126986

Alqahtani, H. M., & Abdullah, M. (2024). A Review on DDoS Attacks Classifying and Detection by ML/DL Models. *International Journal of Advanced Computer Science and Applications*, *15*(2). https://doi.org/10.14569/IJACSA.2024.0150283

Bahashwan, A. A., Anbar, M., Manickam, S., Issa, G., Aladaileh, M. A., Alabsi, B. A., & Rihan, S. D. A. (2024). HLD-DDoSDN: High and low-rates dataset-based DDoS attacks against SDN. *PLOS ONE*, *19*(2), e0297548. https://doi.org/10.1371/journal.pone.0297548

Batool, S., Aslam, M., Akpokodje, E., & Jilani, S. F. (2025). A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments: Machine Learning, Deep Learning, and Federated Learning Perspectives. *Electronics*, *14*(21), 4222. https://doi.org/10.3390/electronics14214222

Chatzoglou, E., Kambourakis, G., Kolias, C., & Smiliotopoulos, C. (2022). Pick Quality Over Quantity: Expert Feature Selection and Data Preprocessing for 802.11 Intrusion Detection Systems. *IEEE Access*, *10*, 64761–64784. https://doi.org/10.1109/ACCESS.2022.3183597

First. (2024). *Common Vulnerability Scoring System: Specification Document*. First.Org. https://www.first.org/cvss/specification-document

Gollier, H., & Vanhoef, M. (2024). SSID Confusion: Making Wi-Fi Clients Connect to the Wrong Network. *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 156–161. https://doi.org/10.1145/3643833.3656126

Hill, W., Acquaah, Y. T., Mason, J., Limbrick, D., Teixeira-Poit, S., Coates, C., & Roy, K. (2024). DDoS in SDN: a review of open datasets, attack vectors and mitigation strategies. *Discover Applied Sciences*, *6*(9), 472. https://doi.org/10.1007/s42452-024-06172-x

Hnamte, V., & Hussain, J. (2024). Enhancing security in Software-Defined Networks: An approach to efficient ARP spoofing attacks detection and mitigation. *Telematics and Informatics Reports*, *14*, 100129. https://doi.org/10.1016/j.teler.2024.100129

Jadhav, S., Thakur, A., Nalbalwar, S., Shah, S., & Chordia, S. (2023). Detection and Mitigation of ARP Spoofing Attack. In *International Conference on Innovative Computing and Communications* (pp. 383–396). https://doi.org/10.1007/978-981-99-3010-4_33

Kampourakis, V., Gkioulos, V., & Katsikas, S. (2023). A systematic literature review on wireless security testbeds in the cyber-physical realm. *Computers & Security*, *133*, 103383. https://doi.org/10.1016/j.cose.2023.103383

Khedr, W. I., Gouda, A. E., & Mohamed, E. R. (2023). P4-HLDMC: A Novel Framework for DDoS and ARP Attack Detection and Mitigation in SD-IoT Networks Using Machine Learning, Stateful P4, and Distributed Multi-Controller Architecture. *Mathematics*, *11*(16), 3552. https://doi.org/10.3390/math11163552

Majumder, S., Deb Barma, M. K., & Saha, A. (2025). ARP spoofing detection using machine learning classifiers: an experimental study. *Knowledge and Information Systems*, *67*(1), 727–766. https://doi.org/10.1007/s10115-024-02219-y

Morsy, S. M., & Nashat, D. (2022). D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing. *IEEE Access*, *10*, 49142–49153. https://doi.org/10.1109/ACCESS.2022.3172329

Mvah, F., Kengne Tchendji, V., Tayou Djamegni, C., Anwar, A. H., Tosh, D. K., & Kamhoua, C. (2024). Countering ARP spoofing attacks in software-defined networks using a game-theoretic approach. *Computers & Security*, *139*, 103696. https://doi.org/10.1016/j.cose.2023.103696

Nasser, H. I., & Hussain, M. A. (2022). Defending a wireless LAN against ARP spoofing attacks using a Raspberry Pi. *Journal of Basrah Researches (Sciences)*, *48*(2), 123–135. https://jou.jobrs.edu.iq/index.php/home/article/view/17

Nazir, R., Laghari, A. A., Kumar, K., David, S., & Ali, M. (2022). Survey on Wireless Network Security. *Archives of Computational Methods in Engineering*, *29*(3), 1591–1610. https://doi.org/10.1007/s11831-021-09631-5

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Prasad, A., & Chandra, S. (2022). Defending ARP Spoofing-based MitM Attack using Machine Learning and Device Profiling. *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 978–982. https://doi.org/10.1109/ICCCIS56430.2022.10037723

Rawia, R., Isa, M. R. M., Ismaila, M. N., Sajak, A. A. B., & Mustafa, A. (2023). Preliminary study: Readiness of WLAN Infrastructure at Malaysian Higher Education Institutes to support Smart Campus Initiative. *JOIV: International Journal on Informatics Visualization*, *7*(3), 945–951. https://doi.org/10.30630/joiv.7.3.1242

Saritakumar, N., Anusuya, K. V., & Krishnakumar, S. (2023). Detection of ARP Spoofing Attacks in Software Defined Networks. *2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)*, 422–426. https://doi.org/10.1109/ICISCoIS56541.2023.10100567

Schepers, D., Ranganathan, A., & Vanhoef, M. (2023). Framing frames: Bypassing Wi-Fi encryption by manipulating transmit queues. *The Proceedings of the 32nd USENIX Security Symposium*, 53–58. https://www.usenix.org/system/files/usenixsecurity23-schepers.pdf

Su, Y., Xiong, D., Qian, K., & Wang, Y. (2024). A Comprehensive Survey of Distributed Denial of Service Detection and Mitigation Technologies in Software-Defined Network. *Electronics*, *13*(4), 807. https://doi.org/10.3390/electronics13040807

Usmani, M., Anwar, M., Farooq, K., Ahmed, G., & Siddiqui, S. (2022). Predicting ARP spoofing with Machine Learning. *2022 International Conference on Emerging Trends in Smart Technologies (ICETST)*, 1–6. https://doi.org/10.1109/ICETST55735.2022.9922925

Wang, W., Xie, Q., Han, Z., Su, C., Rodrigues, J. J. P. C., & Wu, K. (2025). Secure Enhanced IoT-WLAN Authentication Protocol With Efficient Fast Reconnection. *IEEE Transactions on Mobile Computing*, *24*(10), 10085–10098. https://doi.org/10.1109/TMC.2025.3569593

Wijayanto, A., Riadi, I., & Prayudi, Y. (2023). TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *7*(2), 208–217. https://doi.org/10.29207/resti.v7i2.4589