

Software-Defined Networking Approaches for Mitigating IEEE 802.11 Deauthentication and Management-Frame Attacks: A Systematic Literature Review

Geoffrey Mulwa Mutiwa¹, John Gichuki Ndia² Isaac Nyabisa Oteyo³

Abstract: IEEE 802.11 wireless local area networks remain exposed to deauthentication and related management-frame attacks that interrupt service and can support rogue-access-point or interception attacks. Protected Management Frames, wireless intrusion detection systems, and wireless intrusion prevention systems reduce exposure, but residual denial-of-service conditions, sensor dependence, false alarms, and limited network-wide response remain. This systematic literature review assesses how software-defined networking can support mitigation through centralized monitoring, programmable enforcement, dynamic policy control, hybrid detection, programmable data planes, and resilient controllers. A PRISMA 2020-inspired process identified 549 records, removed 96 duplicates, screened 453 records, assessed 126 full texts, and retained 50 studies. Primary screening and extraction were conducted by one reviewer and checked by two co-authors. No disagreements arose. No disagreements arose. Eighteen studies provided direct wireless or management-frame evidence, while 32 provided transferable SDN or software-defined WLAN evidence. Centralized visibility appeared in 22 studies, programmable enforcement in 18, and reactive mitigation in 13. Most evidence came from simulations, emulation, testbeds, surveys, standards, or conceptual architectures rather than production enterprise WLANs. The findings support SDN as a complementary control and response layer, not a proven standalone replacement for protocol-level protection or wireless monitoring. Priority work includes enterprise trials, standardized datasets, controller-resilience testing, explainable detection, Wi-Fi 7 evaluation, and integrated PMF-SDN architectures.

Keywords: Centralized monitoring, Evidence classification, Intrusion prevention, Programmable data planes, Wireless availability

History

Received: 14-05-2026;

Revised: 23-07-2026;

Accepted: 13-08-2026



G. M. Mutiwa

geoffreymutiwa@gmail.com

¹School of Computing and Informatics, Mount Kenya University, P. O. Box 342-01000, Thika– Kenya.

²School of Computing and Information Technology, Murang'a University of Technology, P.O. Box 75-10200, Murang'a, Kenya.

³School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, P.O. Box 62000-00200, Nairobi, Kenya.

1. Introduction

IEEE 802.11 wireless local area networks (WLANs) support enterprise, education, health, industrial, and public-access communication. Their shared radio medium and management procedures create availability and authentication risks that differ from those of wired networks. The IEEE 802.11 base standard defines medium-access and physical-layer operation, while IEEE 802.11w introduced Protected Management Frames (PMF) for selected robust management exchanges [1 - 2]. Early technical studies showed that forged deauthentication and disassociation frames could terminate legitimate

sessions with modest attacker resources [3 - 4]. Later testing showed that deauthentication remains relevant even when modern countermeasures are enabled [5].

Management-frame abuse is not limited to short disconnections. Forced reconnection can support rogue access points, credential capture, malicious frame injection, and multi-channel interception. WPA3 analysis, data-frame injection work, and protected-Wi-Fi man-in-the-middle research show that modern authentication and encryption do not remove all management-plane and implementation risks [6 - 8]. PMF raises the cost of forged robust management frames, but direct studies have reported bypass, deadlock, and denial-of-service conditions (DoS) in WPA2, WPA3, and IEEE 802.11w settings [9 - 11]. Wireless intrusion detection systems (WIDS) and wireless intrusion prevention systems (WIPS) provide sensor-based monitoring, rule matching, rogue-access-point detection, and policy enforcement. Their performance depends on sensor placement, rules, radio coverage, and operational tuning [12 - 13]. Machine-learning models can identify fake access points, sweeping jamming, and deauthentication behaviour, yet their results remain tied to feature selection, training data, class balance, and the traffic environment [14]. These limits support a layered security model rather than reliance on one protection mechanism.

Software-defined networking (SDN) separates forwarding from logically centralized control and allows software applications to install and modify network policy [15]. This architecture provides network-wide telemetry, flow-rule management, traffic redirection, and automated response, but it also introduces controller, interface, and flow-table attack surfaces [16 - 17]. Studies of denial-of-service detection and mitigation in SDN show how centralized measurement and programmable response can support availability protection [18]. WLAN-focused work has applied controller-assisted monitoring and structured wireless defence loops [19 - 20], while broader SDN detection studies provide transferable evidence for early detection and flow-statistics analysis [21 - 22]. Programmable wireless and data-plane work extends these capabilities. A P4-programmable IEEE 802.11 data plane demonstrates that WLAN packet processing can be moved closer to the forwarding path [23]. SDN WLAN architectures

provide centralized control and performance management [24], while P4 security work describes packet inspection and enforcement functions that can operate at line rate [25]. Software-defined wireless architectures, Odin, Ethanol, and Mininet-WiFi show that centralized WLAN control and repeatable wireless experimentation are technically feasible [26 - 29]. More recent work addresses dynamic access control, SD-WLAN implementation, and distributed controller security [30 - 32]. OpenFlow middlebox research further shows how anomaly detection can be coupled to programmable mitigation [33].

The direct WLAN evidence base also contains formal PMF analysis, WPA2 key reinstallation research, WPA3 denial-of-service testing, deauthentication detection, neural management-frame detection, and management-frame protection methods [34 - 39]. Near-direct SD-WLAN studies identify malicious traffic through controller-managed observation [40]. Recent work on low-rate SDN attacks, trustworthy WLAN architecture, control-layer defence, controller flooding, SDN-based intrusion prevention, Internet of Things (IoT)-oriented detection, programmable data-plane security, edge flow-rule attacks, controller placement, and lightweight deep learning extends the transferable evidence base [41 - 50]. Existing surveys discuss SDN security, distributed denial-of-service (DDoS) defense, programmable networks, or software-defined WLAN (SD-WLAN) design, but they do not separate WLAN-specific deauthentication evidence from mechanisms borrowed from wider SDN research. This distinction matters because flow-level DDoS results cannot be treated as direct proof that an SDN controller can identify and stop forged IEEE 802.11 management frames. The problem addressed in this review is therefore the absence of a focused synthesis that states what has been directly tested, what can only be transferred by technical reasoning, and what remains unvalidated.

The review answers four questions, as follows.

RQ1: Which SDN functions have been applied, or have a defensible technical mapping, for mitigating deauthentication and related management-frame attacks?

RQ2: What is the quality and directness of the supporting evidence?

RQ3: How do SDN-based approaches compare with PMF, WIDS, and WIPS in detection, response, scalability, and operational burden?

RQ4: Which research gaps and future directions follow from the current evidence?

The novelty of this review is the explicit separation of direct WLAN evidence from mechanisms transferred from broader programmable-network research. This prevents general SDN findings from being presented as if they were deauthentication experiments.

- Separates direct WLAN or management-frame evidence from transferable SDN, SD-WLAN, P4, and DDoS evidence using explicit decision rules.
- Quantifies publication periods, evidence directness, evaluation settings, detection methods, mitigation functions, and recurring SDN characteristics across the 50-study corpus.
- Compares PMF, WIDS/WIPS, machine-learning detection, SDN control, and programmable data planes without presenting them as interchangeable mechanisms.
- Adds an operational risk assessment covering controller saturation, single-controller failure, rule conflicts, integration cost, interoperability, and migration burden.
- Defines a research programme for enterprise validation, shared WLAN benchmarks, controller resilience, explainable detection, Wi-Fi 7, and hybrid PMF-SDN deployments.

The paper is organized into different sections as follows. Section 2 describes the materials and methods. Section 3 presents the quantitative and thematic results, compares protection mechanisms, interprets the research questions, and reports operational limits, deployment issues, research gaps, and review limitations. Section 4 gives the conclusion and future research directions.

2. Materials and Methods

The review followed a systematic literature review protocol informed by Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 and established software-engineering review guidance [51 - 54]. The protocol was prepared

before full screening and specified the research questions, sources, search concepts, eligibility rules, quality criteria, extraction fields, and synthesis plan. The fixed quantitative corpus contains the 50 studies that passed the stated selection process. Additional methodological references and recent 2024–2026 publications were cited during revision to update context and discussion; they were not added to the closed corpus or used to change the reported frequencies.

The search covered IEEE Xplore, ACM Digital Library, Scopus, SpringerLink, ScienceDirect, and Wiley Online Library. The main Boolean expression combined SDN terms, management-frame or denial-of-service terms, and IEEE 802.11 or WLAN terms: ("software-defined networking" OR SDN OR SD-WLAN) AND ("deauthentication attack" OR "management frame attack" OR disassociation OR DoS) AND ("IEEE 802.11" OR WLAN OR Wi-Fi). Targeted searches added PMF, WPA3 denial of service, WIDS, programmable WLAN, OpenFlow WLAN security, P4 wireless security, controller resilience, and programmable data-plane security. Backward and forward citation checking was used to locate closely related work. Eligible records were peer reviewed, written in English, and addressed IEEE 802.11/WLAN security, SDN security, SD-WLAN architecture, programmable networking, or a mechanism that could be mapped to management-frame mitigation. The review gave priority to DOI-verifiable publications with enough method or architecture detail for extraction. One foundational non-DOI USENIX paper was retained because it documents the practical deauthentication problem. Records were excluded when they lacked WLAN or transferable SDN security relevance, supplied no technical method, duplicated another report, or contained metadata that could not be reconciled. The first author conducted the primary title-and-abstract screening, full-text eligibility assessment, quality appraisal, and data extraction. The second and third authors then checked the inclusion and exclusion decisions, extracted fields, quality judgements, and evidence classifications against the predefined criteria. All checked decisions were confirmed, and no disagreements arose. Because the process used post-screening verification rather than independent blinded duplicate screening, an inter-reviewer kappa statistic

was not calculated. This limitation is stated to avoid overstating the review procedure.

The initial searches produced 549 records. Removal of 96 duplicates left 453 records for title-and-abstract screening. Screening excluded 327 records, leaving 126 full texts. Full-text assessment excluded 76 reports, and 50 studies entered the synthesis. The numerical chain is internally closed: $549 - 96 = 453$; $453 - 327 = 126$; and $126 - 76 = 50$. Each included study was appraised on five domains: method clarity, evaluation support, reproducibility, deployment relevance, and metric reporting. A study received a strong judgement when its architecture or procedure was described, its claims were supported by simulation, emulation, a testbed, measured data, or a documented standard analysis, and its limitations could be identified. The quality assessment informed interpretation rather than acting as an unreported numerical threshold. Data extraction captured publication year, attack focus, WLAN or SDN setting, evidence type, controller or platform, dataset or traffic source, detection logic, mitigation action, evaluation setting, reported metrics, and limitations. The extraction sheet also recorded whether the study measured a management-frame outcome, used an IEEE 802.11 environment, installed or proposed SDN rules, and evaluated controller overhead or resilience.

A study was classified as direct evidence when it measured deauthentication, disassociation, PMF bypass, management-frame denial of service, or WLAN attack detection in an IEEE 802.11 setting and reported a security outcome. A study was classified as transferable evidence when it evaluated an SDN, SD-WLAN, P4, intrusion detection and prevention systems (IDS/IPS), controller-resilience, or DoS mechanism that could be technically mapped to WLAN mitigation but did not directly test the target management-frame attack. When a paper contained both forms, direct classification was used only when the WLAN outcome was measured; otherwise, it remained transferable. A statistical meta-analysis was not suitable because the studies used different attacks, traffic sources, controller platforms, datasets, network sizes, thresholds, and outcome definitions. The synthesis therefore used counts, percentages, structured comparison, and narrative interpretation. No pooled accuracy or latency value was calculated

because doing so would combine non-equivalent measurements.

2.1 Search sources and retrieved records

Table. 1, lists the searched sources, their main focus, and the retrieved-record totals used in the documented selection chain.

Table. 1: Search sources and retrieved records.

Source	Search focus	Records
IEEE Xplore	SDN, WLAN security, wireless networking	148
ACM Digital Library	Wireless attacks, SD-WLAN architectures	74
Scopus	Broad interdisciplinary indexing	126
SpringerLink	WLAN and programmable networking	63
ScienceDirect	Network security and WLAN protection	81
Wiley Online Library	Wireless security and SDN studies	39
Manual citation tracking	Additional related studies	18
Total		549

2.2 Eligibility criteria

Table. 2, states the inclusion and exclusion rules applied during full-text assessment.

Table. 2: Inclusion and exclusion criteria.

Inclusion	Exclusion
Peer-reviewed articles, conference papers, standards, or a directly relevant foundational paper	Non-English, duplicate, non-technical, or unrelated work
WLAN, IEEE 802.11, PMF, deauthentication, management-frame, SDN, SD-WLAN, P4, or transferable DoS-security relevance	No defensible mapping to WLAN or SDN security
Enough method, architecture, or evaluation detail for extraction	Insufficient technical detail
Verifiable metadata and DOI where available	Unresolved metadata mismatch after checking

2.3 Study selection

Fig. 1, presents the numerical path from record identification to the 50 studies retained for synthesis.

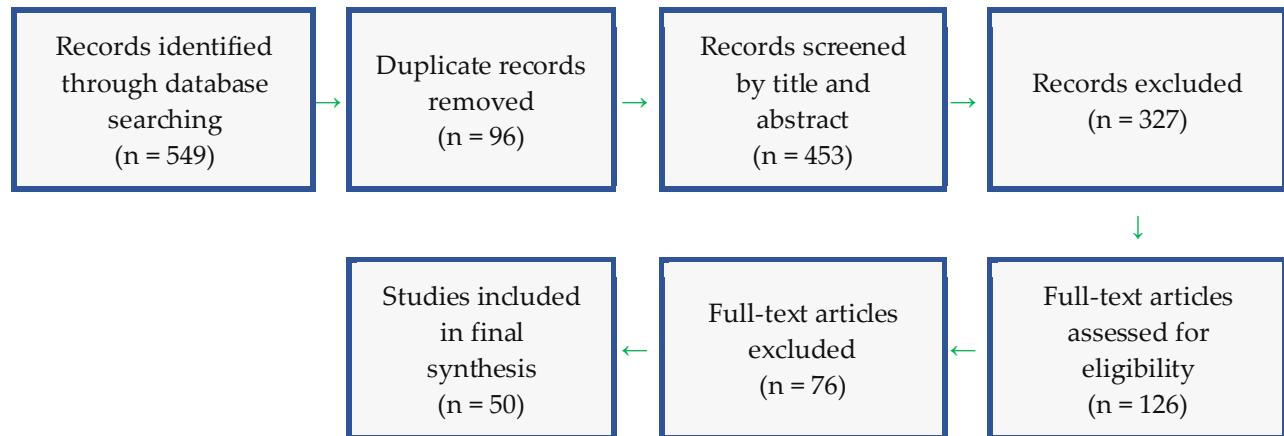


Fig. 1: PRISMA inspired study selection workflow.

2.4 Quality assessment

Table. 3, defines the five quality domains used to judge methodological reporting and deployment relevance.

Table. 3: Quality assessment domains.

Domain	Assessment focus
Method clarity	Architecture, dataset/traffic source, attack model, and procedure described
Evaluation support	Simulation, emulation, testbed, trace, measured dataset, or documented standards analysis
Reproducibility	Tools, settings, features, or steps reported well enough to repeat
Deployment relevance	WLAN realism, network size, mobility, device mix, or operational setting addressed
Metric reporting	Accuracy, false alarms, latency, throughput, overhead, scalability, or recovery reported

2.5 Evidence classification

Table. 4, states the operational classification rules, while Fig. 2, shows the decision path used for direct, transferable, and mixed studies.

Table. 4: Evidence-classification rules.

Evidence type	Decision element	Operational rule
Direct	Target attack	Deauthentication, disassociation, PMF bypass, or management-frame DoS is evaluated
Direct	Environment	IEEE 802.11/WLAN setting or WLAN trace

Direct	Outcome	Attack detection, blocking, continuity, recovery, false alarms, or latency is measured
Transferable	Mechanism	SDN/SD-WLAN/P4/IDS/controller/DoS mechanism has a clear WLAN mitigation role
Transferable	Boundary	No direct management-frame outcome is measured
Mixed paper	Rule	Classify as direct only when the WLAN target outcome is measured; otherwise classify as transferable

3. Results and Discussion

The corpus comprised 50 studies and standards documents. Eighteen studies (36.0%) supplied direct WLAN or management-frame evidence, while 32 (64.0%) supplied transferable SDN or SD-WLAN evidence. The imbalance shows that the field contains more architectural, controller, and flow based work than direct tests of SDN-based deauthentication mitigation. Thirty one studies (62.0%) used simulation, emulation, or a testbed, and 19 (38.0%) were surveys, standards, reviews, or conceptual architectures. Publication activity rose after 2018. The 2021–2023 period contributed 16 studies (32.0%), and 2018–2020 contributed 14 (28.0%). Together, those periods supplied 60.0% of the synthesis corpus. Four foundational studies were published from 2003–2010. Four corpus studies fell in 2024–2025. The low recent count reflects the closed search corpus, not an absence of later publications. Additional recent sources cited later in this section provide contextual support and are not included in the corpus percentages.

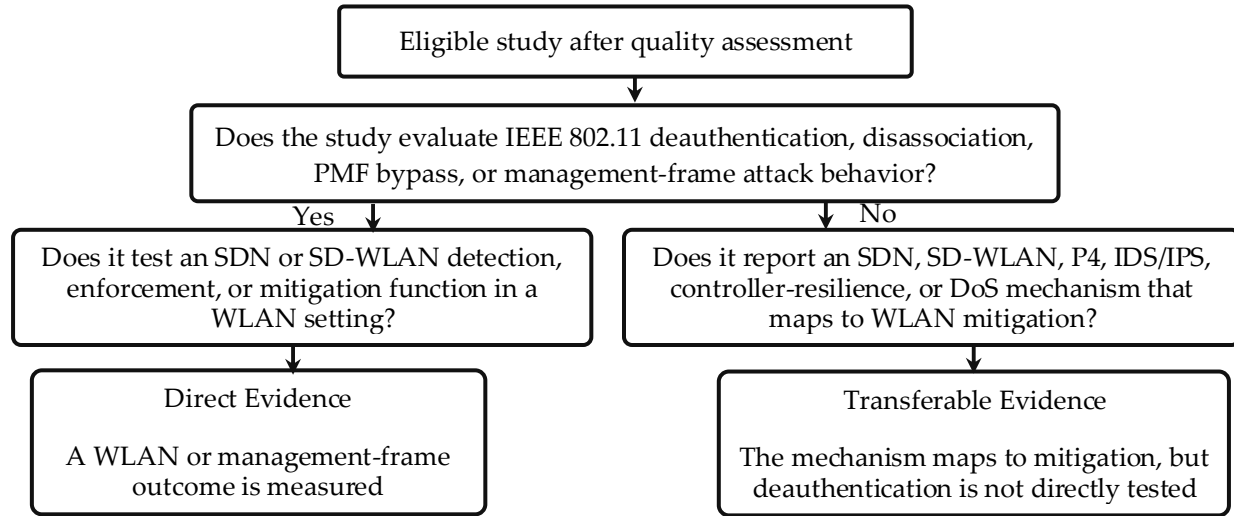


Fig. 2: Decision framework for direct and transferable evidence.

Centralized visibility or control appeared in 22 studies (44.0%), programmable enforcement in 18 (36.0%), reactive or dynamic mitigation in 13 (26.0%), management-frame monitoring in 12 (24.0%), hybrid IDS/WIPS integration in nine (18.0%), controller resilience or placement in five (10.0%), and programmable data-plane or P4 security in four (8.0%). These categories overlap because one study may contribute more than one function. The direct evidence is strongest for the continued feasibility of management-frame attacks, PMF limitations, WPA3 availability weaknesses, and WLAN-specific detection. It supports a clear premise: protocol protection reduces exposure but does not provide network-wide behavioral monitoring or coordinated response. Direct evidence for a fully integrated SDN system that detects forged management frames, decides on a response, applies rules, and validates recovery at enterprise scale remains limited.

The transferable evidence is strongest for controller-managed telemetry, programmable filtering, traffic redirection, anomaly detection, controller protection, and distributed control. OpenFlow and SDN literature [55 - 73] explains how policy can be changed without manual reconfiguration of every forwarding device. P4 work [74 - 77] shows that packet-level features and enforcement can move closer to the data path. These mechanisms provide a technical basis for WLAN mitigation, but the evidence must not be presented as a direct WLAN result when no management-frame test was conducted. Detection methods fell into four broad groups. WIDS/WIPS and

rule-based methods used known frame patterns, thresholds, or policy violations. WLAN machine-learning methods used radio or frame features to classify fake access points, jamming, and deauthentication. Flow-statistics methods used controller telemetry for anomaly identification. Hybrid methods linked sensor observation, classification, controller decisions, and policy enforcement. Recent SDN studies [78 - 89] continue to report machine-learning, deep-learning, statistical, and hierarchical detection methods, but they also repeat concerns about dataset bias, controller overhead, and limited production testing. Mitigation mechanisms included blocking or filtering suspicious traffic, isolating a client or flow, redirecting traffic for inspection, rate limiting, installing higher-priority rules, and protecting controller resources. WLAN-specific enforcement was less common than flow-level SDN response. Programmable data planes can reduce controller round trips for selected checks, but they have limited memory, restricted parsing logic, and platform-specific implementation requirements.

PMF, WIDS/WIPS, and SDN address different control points. PMF protects selected frame exchanges at protocol level. WIDS/WIPS provides radio observation and policy monitoring. SDN supplies network wide correlation and programmable response. The evidence therefore supports layered deployment. A PMF only approach lacks behavioral correlation; a WIDS-only approach may lack coordinated enforcement; an SDN-only approach cannot authenticate a frame that the wireless hardware

never exposes to the controller. The evaluation-setting review responds to the editor's request concerning test-system design. As this article is a literature review, it does not introduce one new experimental system. Instead, the included studies used Mininet or Mininet-WiFi, controller emulation, ns-3 or custom simulation, WLAN testbeds, captured frame traces, benchmark intrusion datasets, and standards or protocol analysis. This variation explains why one pooled accuracy or latency result would be misleading.

3.1 Quantitative profile of the corpus

Table. 5, summarizes evidence directness, evaluation basis, detection approaches, mitigation actions, and controller resilience coverage. Fig. 3 to Fig. 5, visualize the publication pattern, evidence composition, and recurring SDN characteristics.

Table. 5: Quantitative profile of the 50-study corpus.

Dimension	Category	Studies	Share
Evidence directness	Direct WLAN/management-frame evidence	18	36.0%
Evidence directness	Transferable SDN/SD-WLAN evidence	32	64.0%
Evaluation basis	Simulation, emulation, or testbed	31	62.0%
Evaluation basis	Survey, standard, review, or conceptual architecture	19	38.0%
Detection	Rule/WIDS/WIPS oriented	9	18.0%
Detection	Flow-statistics/telemetry	12	24.0%
Detection	Machine Learning/Artificial Intelligence (AI) assisted	7	14.0%
Mitigation	Dynamic blocking/filtering/rule action	14	28.0%
Mitigation	P4/programmed data plane	4	8.0%
Resilience	Controller placement/security	5	10.0%

3.2 Comparison of security mechanisms

Table. 6, compares the best-supported role and main boundary of each security mechanism.

Table. 6: Comparison of WLAN and SDN-enabled security mechanisms.

Mechanism	Best-supported role	Main boundary
PMF	Protocol-level protection for selected robust management frames	No behavioural correlation or network-wide response
WIDS/WIPS	Radio monitoring, rogue-AP detection, rules and alerts	Coverage, tuning, and false alarms
WLAN ML detection	Pattern recognition for deauthentication, jamming, or spoofing	Dataset, feature, drift, and cross-site dependence
SDN control	Shared telemetry, policy coordination, blocking, isolation, redirection	Controller risk, integration burden, radio visibility
P4/data plane	Fast feature extraction and selected enforcement	Hardware limits and little direct WLAN validation

3.3 SDN limitations and deployment controls

Table. 7, links major SDN deployment risks to operational effects and practical controls. Fig. 6, presents the proposed layered architecture.

Table. 7: SDN deployment risks and controls.

Risk	Operational effect	Control
Controller saturation	Event floods delay analysis and rule installation	Rate limiting, edge aggregation, priority queues, resource monitoring
Single controller failure	Defense and network control fail together	Controller replication, local fallback, tested failover
Rule conflict or abuse	Defensive rules interrupt legitimate clients	Signed policy, validation, short-lived rules, rollback
Telemetry gaps	Controller cannot see radio layer evidence	AP/driver hooks, monitor sensors, standardized event export
False alarms	Legitimate roaming or interference triggers blocking	Confidence thresholds, multi-sensor correlation, operator review
Interoperability	Vendor WLAN APIs differ	Open event schema, modular adapters, staged pilots
Cost and migration	New hardware, clusters, training, and operations burden	Incremental deployment, reuse of existing WIDS, cost reporting

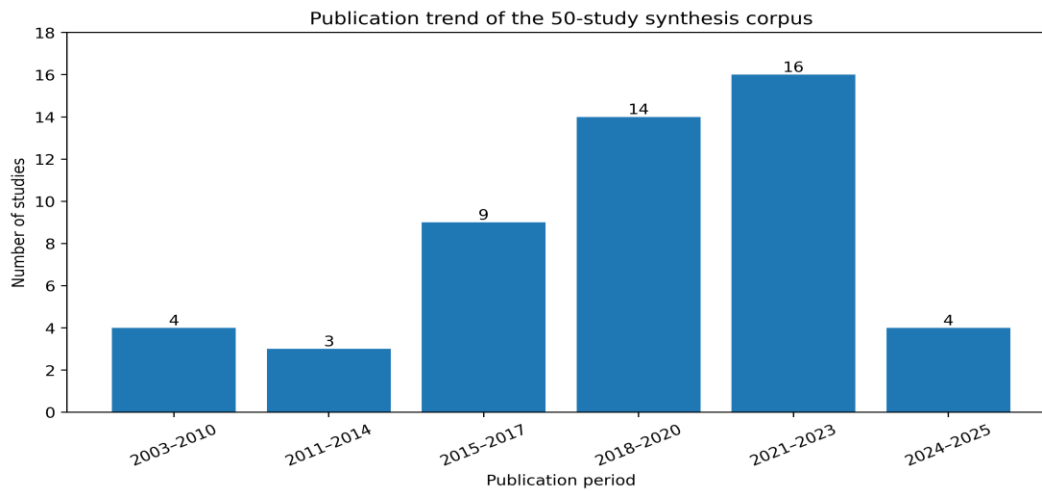


Fig. 3: Publication trend of included studies.

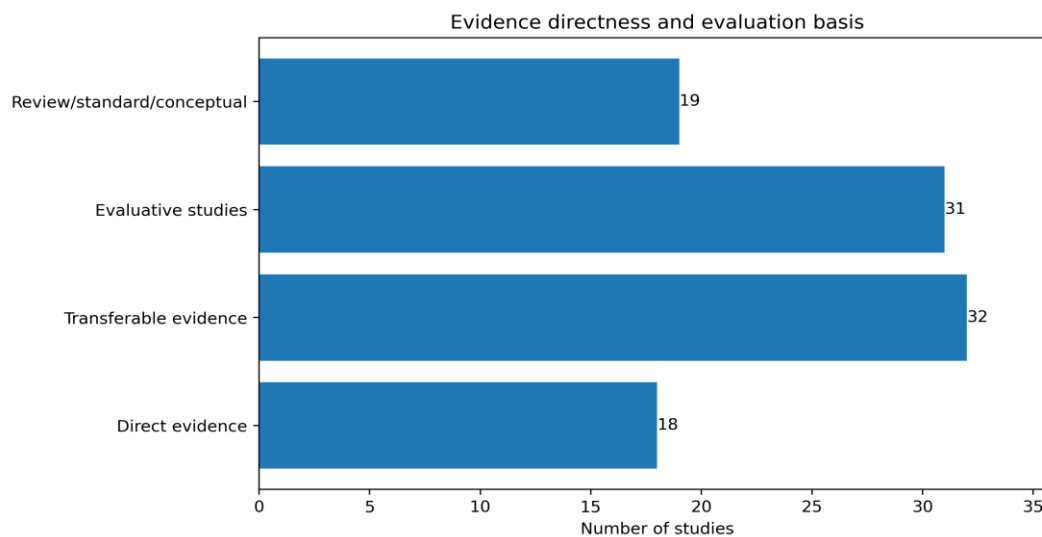


Fig. 4: Evidence directness and evaluation basis.

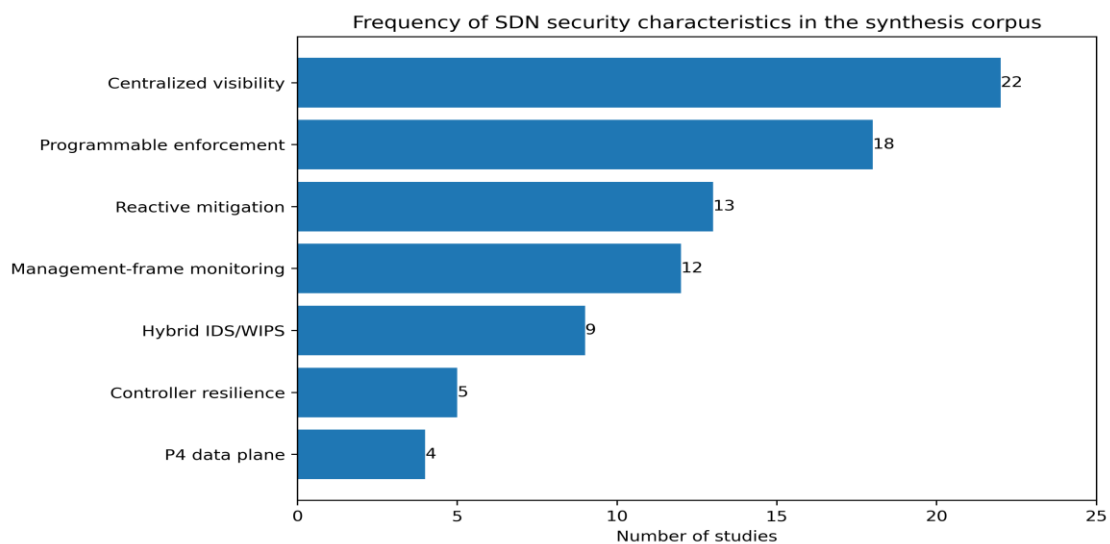


Fig. 5: Frequency of SDN security characteristics.

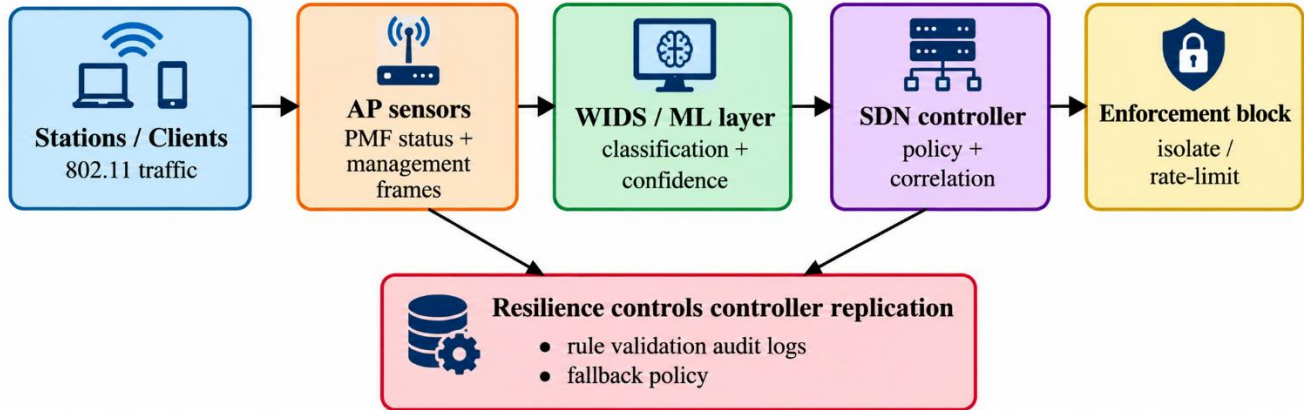


Fig. 6: Proposed hybrid PMF-WIDS/WIPS-SDN mitigation architecture

3.4 Interpretation and comparison

RQ1 is answered by six main capability groups: centralized observation, programmable enforcement, management-frame monitoring, hybrid intrusion detection and prevention, programmable data planes, and controller resilience. Centralized observation is the most frequent capability, but it only becomes useful for deauthentication mitigation when wireless telemetry reaches the controller with enough timing and frame detail. Programmable enforcement is similarly dependent on what the access point, switch, driver, or programmable radio can execute.

RQ2 concerns evidence strength. The direct category supports the attack problem and WLAN detection feasibility. The transferable category supports SDN control and response logic. The evidence does not yet justify a claim that SDN alone has been proven to stop deauthentication across enterprise WLANs. A defensible claim is narrower: SDN can coordinate sensors, correlate events across access points, install policy, isolate suspicious endpoints, protect upstream resources, and support recovery when the wireless infrastructure exposes suitable events and controls.

RQ3 requires a balanced comparison. PMF has low operational latency because protection occurs in the WLAN protocol stack, but its scope is limited to specified robust management frames and implementation behavior. WIDS/WIPS can observe radio events and identify rogue infrastructure, but coverage and false alarms depend on deployment. SDN can apply shared policy across multiple access

points and wired segments, but it adds controller dependencies, southbound and northbound interfaces, rule-management burden, and integration work. No one mechanism dominates every criterion.

The central controller creates a concentration of risk. Packet-in floods, malformed events, topology poisoning, compromised applications, application programming interface (API) misuse, and rule conflicts can affect the same control point used for defence [56 - 66]. Distributed controllers reduce single-node dependence but add synchronization, consistency, trust, and placement problems. Wireless edge placement can lower response delay, yet it increases the number of components that require patching, authentication, logging, and failure handling. Scalability is also a practical constraint. A controller receiving raw management-frame events from many access points may face event bursts during roaming, interference, device churn, or an attack. Feature extraction at the access point or data plane can reduce traffic, but early filtering can discard evidence needed for later investigation. Rate limits and sampling can protect the controller while allowing low-rate attacks to evade detection. Future evaluations should report event rate, controller central processing unit (CPU) and memory use, rule-installation delay, packet loss, client recovery time, and false-alarm cost rather than accuracy alone. Deployment cost is not limited to controller software. Enterprise adoption may require compatible access points, telemetry agents, controller clusters, secure certificates, WIDS sensors, analytics infrastructure, staff training, and staged migration. Vendor APIs and proprietary WLAN control may restrict implementation. A hybrid

design should therefore support fallback operation when the controller is unavailable, local PMF enforcement, signed policy distribution, rule rollback, and audit records. Recent programmable-data-plane studies [74 - 77] support packet-level extraction and low-latency checks, but WLAN management frames are not always visible at a conventional Ethernet switch. Direct use may require programmable access points, driver hooks, radio-monitor interfaces, or an IEEE 802.11-aware data path. The architectural diagram in Figure 6 separates the radio sensor, classification layer, SDN controller, and enforcement point to make this dependency explicit. Recent machine-learning and DDoS studies [78 - 89] also show why reported detection rates need careful interpretation. High scores on benchmark datasets do not establish performance under mobility, changing device populations, encrypted traffic, adversarial evasion, unseen chipset behaviour, or new WLAN standards. Models should be tested across sites and time periods, and results should include precision, recall, F1 score, false-positive rate, detection delay, calibration, resource use, and recovery outcomes. WLAN research from 2024–2026 adds cooperative protected-Wi-Fi intrusion detection, automated 802.11 tools, access-point spoofing detection, traffic analysis for deauthentication, and changing-MAC-address guidance [90 - 95]. These publications show that radio-layer identity, monitoring, and privacy changes remain active concerns. The current IEEE 802.11 revision and Wi-Fi 7 work introduce multi-link operation and denser coordination [96 - 99]. A recent systematic review also reports wide variation in the reported accuracy of machine-learning-based DDoS detection in SDN environments [100]. Future security tests should determine whether an attacker can shift management-frame abuse across links, trigger repeated link changes, overload cross-link telemetry, or exploit inconsistent policy between links.

RQ4 therefore produces seven research gaps. First, few studies test a complete detection-to-recovery chain against management frame attacks. Second, shared and labelled WLAN attack datasets remain limited. Third, controller and access-point overhead are not reported consistently. Fourth, distributed-controller failure and synchronization receive little WLAN-specific testing. Fifth, hybrid PMF-SDN designs are usually proposed rather than

implemented. Sixth, explainable and adversarially tested detection is uncommon. Seventh, Wi-Fi 7 multi-link security has not yet been connected to SDN deauthentication mitigation in a repeatable enterprise experiment. Practical enterprise deployment should begin with PMF enabled where supported, validated WIDS/WIPS coverage, protected controller interfaces, and a narrow set of reversible SDN actions. Automated blocking should use confidence thresholds and short-lived rules until the system is calibrated. Security teams should retain packet or event evidence, log policy changes, and test fallback operation. A controller should not become the only path by which clients can reconnect or by which an administrator can restore service.

This review has limits. The evidence spans protocols, testbeds, datasets, surveys, and simulations, which prevents statistical pooling. The primary screening was completed by one author and checked by two co-authors rather than being independently duplicated from the start. The corpus contains more transferable than direct evidence. Some recent sources are contextual additions rather than members of the fixed quantitative corpus. These boundaries are reported to prevent stronger claims than the data support.

3.5 Research gaps and future work

Table. 8, converts the principal evidence gaps into specific experimental and reporting tasks.

Table. 8: Research gaps and required work.

Gap	Current state	Required work
Complete workflow validation	Few end-to-end tests from frame capture to client recovery	Enterprise testbeds with mobility, device diversity, and repeatable attacks
Shared datasets	Few standardized frame-level corpora	Public labelled traces with PMF, WPA3, jamming, roaming, and benign churn
Controller resilience	Limited WLAN-specific failure testing	Distributed-controller, failover, and saturation experiments
Hybrid PMF-SDN	Mostly architectural proposals	Implemented comparison against PMF-only and WIDS-only baselines
Model trust	Limited cross-site, adversarial, and	Temporal validation, adversarial testing,

	explanation testing	calibrated confidence, human-readable reasons
Programmable wireless data plane	Few direct deauthentication evaluations	P4 or programmable-AP tests with management-frame visibility
Wi-Fi 7	Multi-link security not tied to SDN mitigation	Cross-link attack, policy consistency, and recovery tests

4. Conclusion

This review assessed 50 studies on SDN functions that can support mitigation of IEEE 802.11 deauthentication and related management-frame attacks. Eighteen studies supplied direct WLAN or management-frame evidence, while 32 supplied transferable SDN or SD-WLAN evidence. Centralized visibility, programmable enforcement, reactive response, management-frame monitoring, hybrid intrusion detection, programmable data planes, and controller resilience were the main capability groups. The evidence supports SDN as a coordination and enforcement layer that can work with PMF and WIDS/WIPS. It does not yet support SDN as a fully validated standalone replacement for protocol protection or radio monitoring. For enterprise use, PMF should remain enabled, wireless sensors should cover the radio environment, and SDN actions should be reversible, logged, and protected by controller redundancy and fallback policy. Future studies should test complete detection-to-recovery workflows in dense multi-access-point networks, publish repeatable frame-level datasets, report controller and access-point resource use, and compare false alarms, detection delay, mitigation delay, client recovery, and throughput. Research should also test adversarial and explainable detection, P4-enabled wireless processing, distributed-controller failure, and hybrid PMF-SDN designs. Wi-Fi 7 work should examine multi-link management attacks, cross-link policy consistency, roaming under attack, and coordinated mitigation across 2.4, 5, and 6 GHz links. These steps would move the field from architectural promise toward measured deployment evidence.

Acknowledgment

The first author thanks John Gichuki Ndia and Isaac Nyabisa Oteyo for supervision, screening verification,

quality checking, and manuscript review. The authors also acknowledge institutional support from Mount Kenya University, Murang'a University of Technology, and Jomo Kenyatta University of Agriculture and Technology.

Funding

No external funding was received for this study.

Data Availability Statement

The review data used for the reported counts and synthesis are contained in the article's tables and referenced literature. No proprietary dataset was used.

Conflict of Interest

The authors declare that they have no conflicts of interest.

Ethical Approval

The study did not involve human participants, animals, or personal data collection. Ethical approval was not required.

CRedit Author Contributions

Conceptualization, GM, JN and IO; methodology, GM; software, JN; validation, IO, GM and JN; formal analysis, GM; investigation, IO; resources, JN; data curation, IO; writing—original draft preparation, GM; writing—review and editing, IO; visualization, JN; supervision, JN; project administration, GM; funding acquisition, IO. All authors have read and agreed to the published version of the manuscript.

Declaration on Editorial Tools

No generative artificial intelligence system was used to conduct the literature search, make inclusion decisions, extract data, classify evidence, or create scientific findings. Language and document-preparation assistance used during revision did not replace author responsibility. The authors retain full responsibility for the scientific statements, references, tables, figures, and responses.

References

- [1] "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 802.11-2020 (Revision of IEEE Std 802.11-2016)*, pp. 1 - 4379, February 2021.
<https://doi.org/10.1109/IEEESTD.2021.9363693>
- [2] "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 amendment 4: protected management frames", *IEEE Std 802.11w-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, and IEEE Std 802.11y-2008)* pp. 1 - 111, 30 September 2009.
<https://doi.org/10.1109/IEEESTD.2009.5278657>
- [3] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks", *Computer Standards and Interfaces*, Vol. 31, No. 5, pp. 931–941, 2009.
<https://doi.org/10.1016/j.csi.2008.09.038>
- [4] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions", *Proceedings of the 12th USENIX Security Symposium*, pp. 15–27, 2003. [CrossRef]
- [5] D. Schepers, A. Ranganathan, and M. Vanhoef, "On the robustness of Wi-Fi deauthentication countermeasures", *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 245–256, 2022.
<https://doi.org/10.1145/3507657.3528548>
- [6] M. Vanhoef and E. Ronen, "Dragonblood: analyzing the dragonfly handshake of WPA3 and EAP-PWD", *2020 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, pp. 517-533, 2020.
<https://doi.org/10.1109/SP40000.2020.00031>
- [7] W. Kim, S. Kim, and H. Lim, "Malicious data frame injection attack without seizing association in IEEE 802.11 wireless LANs", *IEEE Access*, Vol. 9, pp. 16649-16660, 2021.
<https://doi.org/10.1109/ACCESS.2021.3054130>
- [8] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "Multi-channel man in the middle attacks against protected Wi-Fi networks: A state-of-the-art review", *Expert Systems with Applications*, Vol. 210, art. no. 118401, 2022.
<https://doi.org/10.1016/j.eswa.2022.118401>
- [9] K. Lounis, S. H. H. Ding, and M. Zulkernine, "Cut It: Deauthentication attacks on protected management frames in WPA2 and WPA3", *Foundations and Practice of Security*, pp. 235–252, 2022.
https://doi.org/10.1007/978-3-031-08147-7_16
- [10] E. Chatzoglou, G. Kambourakis, and C. Koliass, "How is your Wi-Fi connection today? DoS attacks on WPA3-SAE", *Journal of Information Security and Applications*, Vol. 64, art. no. 103058, 2022.
<https://doi.org/10.1016/j.jisa.2021.103058>
- [11] C. Liu and J. Qiu, "Performance study of 802.11w for preventing DoS attacks on wireless local area networks", *Wireless Personal Communications*, Vol. 95, pp. 1031–1053, 2017.
<https://doi.org/10.1007/s11277-016-3812-9>
- [12] S. C. Sethuraman, S. Dhamodaran, and V. Vijayakumar, "Intrusion detection system for detecting wireless attacks in IEEE 802.11 networks", *IET Networks*, Vol. 8, No. 4, pp. 219–232, 2019.
<https://doi.org/10.1049/iet-net.2018.5050>
- [13] N. Dalal, N. Akhtar, A. Gupta, N. Karamchandani, G. S. Kasbekar, and J. Parekh, "A wireless intrusion detection system for 802.11 WPA3 networks", *2022 14th International Conference on COMMunication Systems & NETworkS (COMSNETS)*, Bangalore, India, pp. 384-392, 2022.
<https://doi.org/10.1109/COMSNETS53615.2022.9668542>
- [14] A. Amoordon, V. Deniau, A. Fleury, and C. Gransart, "A single supervised learning model to detect fake access points, frequency sweeping jamming and deauthentication attacks in IEEE 802.11 networks", *Machine Learning with Applications*, Vol. 10, art. no. 100389, 2022.
<https://doi.org/10.1016/j.mlwa.2022.100389>
- [15] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software defined networking: a

- comprehensive survey", *Proceedings of the IEEE*, Vol. 103, No. 1, pp. 14-76, 2015.
<https://doi.org/10.1109/JPROC.2014.2371999>
- [16] I. Ahmad, S. Namal, M. Ylianttila and A. Gurtov, "Security in software defined networks: a survey", *IEEE Communications Surveys and Tutorials*, Vol. 17, No. 4, pp. 2317-2346, Fourth quarter 2015.
<https://doi.org/10.1109/COMST.2015.2474118>
- [17] S. Scott-Hayward, S. Natarajan and S. Sezer, "A survey of security in software defined networks", *IEEE Communications Surveys and Tutorials*, Vol. 18, No. 1, pp. 623-654, 2016.
<https://doi.org/10.1109/COMST.2015.2453114>
- [18] L. F. Eliyan and R. D. Pietro, "DoS and DDoS attacks in software defined networks: A survey of existing solutions and research challenges", *Future Generation Computer Systems*, Vol. 122, pp. 149-171, 2021.
<https://doi.org/10.1016/j.future.2021.03.011>
- [19] R. Cwalinski and H. Koenig, "SDN based attack detection in wireless local area networks", *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, Montreal, QC, Canada, pp. 207-211, 2018.
<https://doi.org/10.1109/NETSOFT.2018.8460121>
- [20] P. Zanna, P. Radcliffe, and D. Kumar, "Preventing attacks on wireless networks using SDN-controlled OODA loops and cyber kill chains", *Sensors*, Vol. 22, No. 23, art. no. 9481, 2022.
<https://doi.org/10.3390/s22239481>
- [21] P. Manso, J. Moura, and C. Serrão, "SDN-based intrusion detection system for early detection and mitigation of DDoS attacks", *Information*, Vol. 10, No. 3, art. no. 106, 2019.
<https://doi.org/10.3390/info10030106>
- [22] Y. Xu and Y. Liu, "DDoS attack detection under SDN context", *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, San Francisco, CA, USA, pp. 1-9, 2016.
<https://doi.org/10.1109/INFOCOM.2016.7524500>
- [23] P. Zanna, P. Radcliffe and D. Kumar, "WP4: A P4 programmable IEEE 802.11 data plane", *2020 30th International Telecommunication Networks and Applications Conference (ITNAC)*, Melbourne, VIC, Australia, pp. 1-6, 2020.
<https://doi.org/10.1109/ITNAC50341.2020.9315141>
- [24] K. Košťál, R. Bencel, M. Ries, P. Trúchly, and I. Kotuliak, "High performance SDN WLAN architecture", *Sensors*, Vol. 19, No. 8, art. no. 1880, 2019.
<https://doi.org/10.3390/s19081880>
- [25] A. AlSabeih, J. Khoury, E. Kfoury, J. Crichigno, and E. Bou-Harb, "A survey on security applications of P4 programmable switches and a STRIDE-based vulnerability assessment", *Computer Networks*, Vol. 207, art. no. 108800, 2022.
<https://doi.org/10.1016/j.comnet.2022.108800>
- [26] C. J. Bernardos, A. de la Oliva, P. Serrano, A. Banchs, L. M. Contreras, H. Jin, and J. C. Zúñiga, "An architecture for software defined wireless networking", *IEEE Wireless Communications*, Vol. 21, No. 3, pp. 52-61, 2014.
<https://doi.org/10.1109/MWC.2014.6845049>
- [27] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, and T. Vazao, "Towards programmable enterprise WLANs with Odin", *Proceedings of the first Workshop on Hot topics in Software Defined Networks*, pp. 115-120, 2012.
<https://doi.org/10.1145/2342441.2342465>
- [28] H. Moura, A. R. Alves, J. R. A. Borges, D. F. Macedo, and M. A. M. Vieira, "Ethanol: A software defined wireless networking architecture for IEEE 802.11 networks", *Computer Communications*, Vol. 149, pp. 176 - 188, 2020.
<https://doi.org/10.1016/j.comcom.2019.10.010>
- [29] R. R. Fontes, S. Afzal, S. H. B. Brito, M. A. S. Santos and C. E. Rothenberg, "Mininet-WiFi: Emulating software defined wireless networks", *2015 11th International Conference on Network and Service Management (CNSM)*, Barcelona, Spain, pp. 384 - 389, 2015.
<https://doi.org/10.1109/CNSM.2015.7367387>
- [30] H. A. Oulahyane, A. Bahnasse, A. Bakali, S. Broumi, I. M. El-Hasnony, and M. Talea, "Secure model for dynamic access control and unreliable access point detection: Improving QoS through SDN in wireless networks", *SN Computer Science*, Vol. 5, art. no. 88, 2024.
<https://doi.org/10.1007/s42979-023-02407-7>
- [31] K. I. Qureshi, L. Wang, L. Sun, C. Zhu and L. Shu, "A review on design and implementation

- of software defined WLANs", *IEEE Systems Journal*, Vol. 14, No. 2, pp. 2601-2614, June 2020.
<https://doi.org/10.1109/JSYST.2019.2960400>
- [32] N. S. Shaji and R. Muthalagu, "Survey on security aspects of distributed software-defined networking controllers in an enterprise SD-WLAN", *Digital Communications and Networks*, Vol. 10, No. 6, pp. 1716–1731, 2024.
<https://doi.org/10.1016/j.dcan.2023.09.004>
- [33] K. Giotis, G. Androulidakis, and B. S. Maglaris, "A scalable anomaly detection and mitigation architecture for legacy networks via an OpenFlow middlebox", *Security and Communications Networks*, Vol. 9, No. 13, pp. 1958 – 1970, 2016.
<https://doi.org/10.1002/sec.1368>
- [34] M. Eian and S. F. Mjøl̂snes, "A formal analysis of IEEE 802.11w deadlock vulnerabilities", *2012 Proceedings IEEE INFOCOM*, Orlando, FL, USA, pp. 918 - 926, 2012.
<https://doi.org/10.1109/INFCOM.2012.6195841>
- [35] M. Vanhoef and P. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2", *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1313–1328, 2017.
<https://doi.org/10.1145/3133956.3134027>
- [36] K. Lounis and M. Zulkernine, "Bad-Token: Denial of service attacks on WPA3," *Proceedings of the 12th International Conference on Security of Information and Networks*, pp. 1–8, 2019.
<https://doi.org/10.1145/3357613.3357629>
- [37] R. Korolkov, S. Kutsak, and V. Voskoboinyk, "Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection", *Bulletin of V.N. Karazin Kharkiv National University, Series «Mathematical Modeling. Information Technology. Automated Control Systems*, Vol. 50, pp. 58–70, 2021.
<https://doi.org/10.26565/2304-6201-2021-50-06>
- [38] A. E. Abdallah, M. Hamdan, M. S. M. Gismalla, A. O. Ibrahim, N. S. Aljurayban, W. Nagmeldin, and M. H. H. Khairi, "Detection of management-frames-based denial-of-service attack in wireless LAN networks using an artificial neural network", *Sensors*, Vol. 23, No. 5, art. no. 2663, 2023.
<https://doi.org/10.3390/s23052663>
- [39] W. Ge, J. Li, and S. Sampalli, "Prevention of management frame attacks on 802.11 WLANs", *International Journal of Wireless and Mobile Computing*, Vol. 3, No. 3, pp. 133–144, 2009.
<https://doi.org/10.1504/IJWMC.2009.028895>
- [40] R. Cwalinski and H. Koenig, "Identifying malicious traffic in software defined wireless local area networks", *2018 International Conference on Computing, Networking and Communications (ICNC)*, Maui, HI, USA, pp. 195–199, 2018.
<https://doi.org/10.1109/ICNC.2018.8390307>
- [41] J. Wang and L. Wang, "LR-STGCN: Detecting and mitigating low-rate DDoS attacks in SDN based on a spatial-temporal graph neural network", *Computers & Security*, Vol. 154, art. no. 104460, 2025.
<https://doi.org/10.1016/j.cose.2025.104460>
- [42] Y. Liu, T. Guan, J. Zhang, D. Liang, and Q. Guan, "Design and optimization of an integrated and trustworthy WLAN network architecture based on SDN for power systems", *Proceedings of the 2024 International Conference on Cloud Computing and Big Data*, pp. 86–92, 2024.
<https://doi.org/10.1145/3695080.3695095>
- [43] M. Elhejazi, and M. Musbah, "Dynamic defense-in-depth model for the SDN control layer to improve OpenFlow protocol security", *The 7th International Conference on Engineering & MIS 2021*, pp. 1–7, 2021.
<https://doi.org/10.1145/3492547.3492625>
- [44] H. Wang, L. Xu and G. Gu, "FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks", *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Rio de Janeiro, Brazil, pp. 239-250, 2015.
<https://doi.org/10.1109/DSN.2015.27>
- [45] N. Mazhar, R. Salleh, M. A. Hossain, and M. Zeeshan, "SDN based intrusion detection and prevention systems using manufacturer usage description: A survey", *International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 12, art. no. 83, 2020.
<https://doi.org/10.14569/IJACSA.2020.0111283>
- [46] A. A. Alashhab, M. S. M. Zahid, A. Muneer, and M. Abdullahi, "Low-rate DDoS attack detection using deep learning for SDN-enabled IoT networks", *International Journal of Advanced*

- Computer Science and Applications*, Vol. 13, No. 11, art. no. 41, 2022.
<https://doi.org/10.14569/IJACSA.2022.0131141>
- [47] Y. Gao and Z. Wang, "A review of P4 programmable data planes for network security", *Mobile Information Systems*, Vol. 2021, No. 1, art. no. 1257046, 2021.
<https://doi.org/10.1155/2021/1257046>
- [48] S. S. Baidya and R. Hewett, "SDN-based edge computing security: Detecting and mitigating flow rule attacks", *Proceedings of the 4th ACM/IEEE Symposium on Edge Computing*, pp. 364 – 370, 2019.
<https://doi.org/10.1145/3318216.3363374>
- [49] Q. Qin, K. Poularakis, G. Iosifidis, S. Kompella and L. Tassiulas, "SDN controller placement with delay overhead balancing in wireless edge networks", *IEEE Transactions on Network and Service Management*, Vol. 15, No. 4, pp. 1446-1459, December 2018.
<https://doi.org/10.1109/TNSM.2018.2876064>
- [50] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martínez-del-Rincón and D. Siracusa, "Lucid: a practical, lightweight deep learning solution for DDoS attack detection", *IEEE Transactions on Network and Service Management*, Vol. 17, No. 2, pp. 876-889, June 2020.
<https://doi.org/10.1109/TNSM.2020.2971776>
- [51] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews", *BMJ*, Vol. 372, art. no. 71, 2021.
<https://doi.org/10.1136/bmj.n71>
- [52] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—A systematic literature review", *Information and Software Technology*, Vol. 51, No. 1, pp. 7–15, 2009.
<https://doi.org/10.1016/j.infsof.2008.09.009>
- [53] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering", *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, pp. 1–10, 2014.
<https://doi.org/10.1145/2601248.2601268>
- [54] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update", *Information and Software Technology*, Vol. 64, pp. 1–18, 2015.
<https://doi.org/10.1016/j.infsof.2015.03.007>
- [55] N. McKeown et al., "OpenFlow: Enabling innovation in campus networks", *ACM SIGCOMM Computer Communication Review*, Vol. 38, No. 2, pp. 69–74, 2008.
<https://doi.org/10.1145/1355734.1355746>
- [56] B. A. A. Nunes, M. Mendonca, X. -N. Nguyen, K. Obraczka and T. Turletti, "A survey of software-defined networking: past, present, and future of programmable networks", *IEEE Communications Surveys & Tutorials*, Vol. 16, No. 3, pp. 1617-1634, 2014.
<https://doi.org/10.1109/SURV.2014.012214.00180>
- [57] D. B. Rawat and S. R. Reddy, "Software defined networking architecture security and energy efficiency: a survey", *IEEE Communications Surveys & Tutorials*, Vol. 19, No. 1, pp. 325-346, 2017.
<https://doi.org/10.1109/COMST.2016.2618874>
- [58] M. Dabbagh, B. Hamdaoui, M. Guizani and A. Rayes, "Software-defined networking security: pros and cons", *IEEE Communications Magazine*, Vol. 53, No. 6, pp. 73-79, June 2015.
<https://doi.org/10.1109/MCOM.2015.7120048>
- [59] I. Alsmadi and D. Xu, "Security of software defined networks: A survey", *Computers & Security*, Vol. 53, pp. 79–108, 2015.
<https://doi.org/10.1016/j.cose.2015.05.006>
- [60] R. Sahay, W. Meng, and C. D. Jensen, "The application of software defined networking on securing computer networks: A survey", *Journal of Network and Computer Applications*, Vol. 131, pp. 89–108, 2019.
<https://doi.org/10.1016/j.jnca.2019.01.019>
- [61] W. Li, W. Meng, and L. F. Kwok, "A survey on OpenFlow-based software defined networks: Security challenges and countermeasures", *Journal of Network and Computer Applications*, Vol. 68, pp. 126–139, 2016.
<https://doi.org/10.1016/j.jnca.2016.04.011>
- [62] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, "Security in SDN: A survey", *Journal of Network and Computer Applications*, Vol. 159, art. no. 102595, 2020.
<https://doi.org/10.1016/j.jnca.2020.102595>
- [63] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A review, research

- challenges and future directions", *Computer Science Review*, Vol. 37, art. no. 100279, 2020.
<https://doi.org/10.1016/j.cosrev.2020.100279>
- [64] S. Kaur, K. Kumar, N. Aggarwal, and G. Singh, "A survey of DDoS defence solutions in SDN: Taxonomy, research challenges, and future directions", *Computers & Security*, Vol. 110, art. no. 102423, 2021.
<https://doi.org/10.1016/j.cose.2021.102423>
- [65] R. Deb and S. Roy, "A survey of vulnerability and information security in software-defined networking", *Computer Networks*, Vol. 206, art. no. 108802, 2022.
<https://doi.org/10.1016/j.comnet.2022.108802>
- [66] B. Ayodele and V. Buttigieg, "SDN as a defence mechanism: A survey", *International Journal of Information Security*, Vol. 23, pp. 141–185, 2024.
<https://doi.org/10.1007/s10207-023-00764-1>
- [67] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDoS attack detection in software defined networking", *Journal of Network and Computer Applications*, Vol. 187, art. no. 103108, 2021.
<https://doi.org/10.1016/j.jnca.2021.103108>
- [68] A. AlEroud and I. Alsmadi, "Identifying cyber-attacks on software defined networks: An inference based intrusion detection approach", *Journal of Network and Computer Applications*, Vol. 80, pp. 152–164, 2017.
<https://doi.org/10.1016/j.jnca.2016.12.024>
- [69] K. K. Karmakar, V. Varadarajan, and U. Tupakula, "Mitigating attacks in software defined networks", *Cluster Computing*, Vol. 22, pp. 1143–1157, 2019.
<https://doi.org/10.1007/s10586-018-02900-2>
- [70] A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck, "Software defined networking for security improvement in wireless mobile networks", *Computer Networks*, Vol. 66, pp. 94–101, 2014.
<https://doi.org/10.1016/j.comnet.2014.03.009>
- [71] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security", *Mobile Networks and Applications*, Vol. 21, pp. 729–743, 2016.
<https://doi.org/10.1007/s11036-015-0665-5>
- [72] A. Gudipati, D. Perry, L. E. Li, and S. Katti, "SoftRAN: Software defined radio access network", *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pp. 25–30, 2013.
<https://doi.org/10.1145/2491185.2491207>
- [73] L. E. Li, Z. M. Mao and J. Rexford, "Toward software defined cellular networks", *2012 European Workshop on Software Defined Networking*, Darmstadt, Germany, pp. 7–12, 2012.
<https://doi.org/10.1109/EWSDN.2012.28>
- [74] P. Bosshart et al., "P4: Programming protocol-independent packet processors", *ACM SIGCOMM Computer Communication Review*, Vol. 44, No. 3, pp. 87–95, 2014.
<https://doi.org/10.1145/2656877.2656890>
- [75] R. Doriguzzi-Corin, L. A. D. Knob, L. Mendozzi, D. Siracusa, and M. Savi, "Introducing packet-level analysis in programmable data planes to advance network intrusion detection", *Computer Networks*, Vol. 239, art. no. 110162, 2024.
<https://doi.org/10.1016/j.comnet.2023.110162>
- [76] A. Mazloun, A. AlSabeh, E. Kfoury, and J. Crichigno, "Security applications in P4: Implementation and lessons learned", *Computer Networks*, Vol. 257, art. no. 111011, 2025.
<https://doi.org/10.1016/j.comnet.2024.111011>
- [77] M. E. Şahin and M. Demirci, "HELP4DNS: Leveraging the programmable data plane for effective and robust defense against DDoS attacks on DNS", *Journal of Network and Computer Applications*, Vol. 240, art. no. 104198, 2025.
<https://doi.org/10.1016/j.jnca.2025.104198>
- [78] A. I. Hassan, E. A. E. Reheem, and S. K. Guirguis, "An entropy and machine learning based approach for DDoS attacks detection in software defined networks", *Scientific Reports*, Vol. 14, art. no. 18159, 2024.
<https://doi.org/10.1038/s41598-024-67984-w>
- [79] H. A. Butt, K. S. A. Harthy, M. A. Shah, M. Hussain, R. Amin, and M. U. Rehman, "Enhanced DDoS detection using advanced machine learning and ensemble techniques in software defined networking", *Computers, Materials and Continua*, Vol. 81, No. 2, pp. 3003–3031, 2024.
<https://doi.org/10.32604/cmc.2024.057185>
- [80] D. Han, H. Li, X. Fu, and S. Zhou, "Traffic feature selection and distributed denial-of-service attack detection in software defined

- networks based on machine learning", *Sensors*, Vol. 24, No. 13, art. no. 4344, 2024.
<https://doi.org/10.3390/s24134344>
- [81] S. Kaur, K. Kumar, and N. Aggarwal, "Enhancing DDoS defense in SDN using hierarchical machine learning models", *Journal of Network and Computer Applications*, Vol. 239, art. no. 104168, 2025.
<https://doi.org/10.1016/j.jnca.2025.104168>
- [82] M. Yue, H. Yan, R. Han, and Z. Wu, "A DDoS attack detection method based on IQR and DFFCNN in SDN", *Journal of Network and Computer Applications*, Vol. 240, art. no. 104203, 2025.
<https://doi.org/10.1016/j.jnca.2025.104203>
- [83] D. Kalambe, D. Sharma, P. Kadam, and S. Surati, "A comprehensive plane-wise review of DDoS attacks in SDN: Leveraging detection and mitigation through machine learning and deep learning", *Journal of Network and Computer Applications*, Vol. 235, art. no. 104081, 2025.
<https://doi.org/10.1016/j.jnca.2024.104081>
- [84] I. Varalakshmi and M. Thenmozhi, "Entropy based earlier detection and mitigation of DDOS attack using stochastic method in SDN-IOT", *Measurement*, Vol. 39, art. no. 101873, 2025.
<https://doi.org/10.1016/j.measen.2025.101873>
- [85] W. Wang, Y. Liu, Q. Meng, and Z. Chen, "DDoS attack detection and defense techniques in software defined networks: A survey", *Computer Science Review*, Vol. 60, art. no. 100921, 2026.
<https://doi.org/10.1016/j.cosrev.2026.100921>
- [86] B. Shyryn, T. A. Ahanger, and A. Zhumadillayeva, "Enhancing software-defined network security with deep learning: A comprehensive review", *International Journal of Information Security*, Vol. 25, art. no. 66, 2026.
<https://doi.org/10.1007/s10207-026-01232-2>
- [87] S. Ganeshan and R. K. Ramasamy, "A systematic review of machine-learning-based detection of DDoS attacks in software-defined networks", *Future Internet*, Vol. 18, No. 2, art. no. 109, 2026.
<https://doi.org/10.3390/fi18020109>
- [88] O. Polat, Ö. Durmuş, F. Doğan, M. Türkoğlu, H. Şeker, F. Atasoy, and E. Algül, "Supervised and deep learning techniques for DDoS detection in software-defined network architectures: A systematic review", *Engineering Science and Technology an International Journal*, Vol. 75, art. no. 102290, 2026.
<https://doi.org/10.1016/j.jestch.2026.102290>
- [89] Z. You, L. Mai, S. Suo, Q. Lin, and Z. Xiong, "In-depth analysis of DDoS anomaly detection in software defined networks", *Journal of Wireless Communications and Networking*, 2026.
<https://doi.org/10.1186/s13638-026-02630-9>
- [90] M. Thankappan, H. Rifà-Pous and C. Garrigues, "A signature-based wireless intrusion detection system framework for multi channel man in the middle attacks against protected Wi-Fi networks", *IEEE Access*, Vol. 12, pp. 23096-23121, 2024.
<https://doi.org/10.1109/ACCESS.2024.3362803>
- [91] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "A distributed and cooperative signature-based intrusion detection system framework for multi-channel man in the middle attacks against protected Wi-Fi networks", *International Journal of Information Security*, Vol. 23, pp. 3527-3546, 2024.
<https://doi.org/10.1007/s10207-024-00899-9>
- [92] D. Koutras, P. Dimitrellos, P. Kotzanikolaou, and C. Douligeris, "Automated Wi-Fi intrusion detection tool on 802.11 networks", *ITU Journal Future and Evolving Technologies*, Vol. 5, No. 1, pp. 88-103, 2024.
<https://doi.org/10.52953/LHXO3338>
- [93] J. Machaj, C. Safon, S. Matúška, and P. Brída, "Detection of access point spoofing in the wi-fi fingerprinting based positioning", *Sensors*, Vol. 24, No. 23, art. no. 7624, 2024.
<https://doi.org/10.3390/s24237624>
- [94] F. Ertam and O. Aydogmus, "Privacy preserving detection of Wi-Fi deauthentication attacks on robotic systems using temporal traffic features", *IEEE Access*, Vol. 14, pp. 46634-46649, 2026.
<https://doi.org/10.1109/ACCESS.2026.3677527>
- [95] J. Henry and Y. Lee, "Randomized and changing media access control (MAC) addresses: context, network impacts, and use cases", *RFC 9797*, June 2025.
<https://doi.org/10.17487/RFC9797>
- [96] "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 - amendment 4: enhancements for wireless LAN sensing", *IEEE Std 802.11bf-2025 (Amendment to IEEE 802.11-2024, as amended by IEEE 802.11bh-2024, IEEE 802.11be-2024, and IEEE 802.11bk-2025)*, pp. 1-228, September 2025.
<https://doi.org/10.1109/IEEESTD.2025.11184214>
- [97] E. Khorov, I. Levitsky, and I. F. Akyildiz, "Current status and directions of IEEE 802.11be, the future Wi-Fi 7", *IEEE Access*, Vol. 8, pp. 88664–88688, 2020.
<https://doi.org/10.1109/ACCESS.2020.2993448>
- [98] S. Avallone, P. Imputato, and F. Marrone, "Exploiting multiple links with a single interface: A performance study", *Ad Hoc Networks*, Vol. 180, art. no. 104029, 2026.
<https://doi.org/10.1016/j.adhoc.2025.104029>
- [99] R. G. Sangeetha, C. Hemanth, K. T. Ankitha, and A. Jaiswal, "IEEE 802.11Be WLANs: Performance assessment of multi link operation with unsaturated queues", *Computer Networks*, Vol. 281, art. no. 112187, 2026.
<https://doi.org/10.1016/j.comnet.2026.112187>
- [100] E. A. A. Mandhari, M. Abdulnabi, R. J. Lontok, and A. Ali, "A systematic literature review on the accuracy of machine learning based DDoS detection techniques in software defined networking", *Discover Computing*, Vol. 29, art. no. 147, 2026.
<https://doi.org/10.1007/s10791-026-10050-y>



Copyright: © 2026 by the authors, Licensee ITEECS, India. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).
