Brief Report

Security Vulnerabilities in WLAN: EmergingAttacks and Defensive Mechanisms

Arimondo Scrivano *

Posted Date: 20 June 2025

doi: 10.20944/preprints202506.1688.v1

Keywords: Denial of Service (DoS); Man-in-the-Middle (MitM); Wireless Local Area Networks (WLANs)

 doi:10.20944/preprints202506.1688.v1

Brief Report

Security Vulnerabilities in WLAN: Emerging Attacks and Defensive Mechanisms

Arimondo Scrivano

[1] DEIB, Dipartimento di Elettronica, Informazione e Bioingegneria; arimondo.scrivano@mail.polimi.it
[2] Politecnico di Milano

Abstract

Wireless Local Area Networks (WLANs) have become integral to modern communication infrastructure, providing unparalleled mobility and convenience. However, their pervasiveness has made them attractive targets for malicious entities. This article offers a comprehensive review of the evolving landscape of security vulnerabilities within WLANs, examining both the traditional and emerging attack vectors. Specifically, we discuss the exploitation of the IEEE 802.11 protocol and its derivations, highlighting common threats such as Denial of Service (DoS), Man-in-the-Middle (MitM), and rogue access points. Additionally, we address novel attack trends, including side-channel attacks and vulnerabilities arising from the proliferation of the Internet of Things (IoT) devices in WLAN environments. Furthermore, this review delves into state-of-the-art defensive mechanisms, encompassing advancements in encryption, authentication protocols, anomaly-based intrusion detection systems, and machine learning approaches designed to fortify WLAN architectures against sophisticated attacks. By identifying key research gaps and proposing future directions, this article aims to aid researchers and practitioners in developing robust WLAN security paradigms.

Keywords: Denial of Service (DoS); man-in-the-middle (MitM); wireless local area networks (WLANs)

1. Introduction

The transformative impact of Wireless Local Area Networks (WLANs) on modern communication paradigms cannot be overstated, as they provide unparalleled mobility and resource accessibility. By eliminating dependency on physical cabling, WLANs have entrenched themselves as an essential component in a myriad of settings, ranging from corporate environments to residential areas and public hotspots [1,2]. However, this technological leap forward has concurrently ushered in a multifaceted spectrum of security challenges that necessitate continuous vigilance and inventive solutions.

A paramount concern within WLAN security is the assurance of data confidentiality and integrity. The IEEE 802.11 standard, which underpins WLAN functionality, has undergone numerous revisions aimed at countering evolving threat landscapes. Early cryptographic mechanisms such as Wired Equivalent Privacy (WEP) were eventually deemed insecure due to inherent flaws like static key usage and weak initialization vectors, which rendered them susceptible to the Fluhrer, Mantin, and Shamir (FMS) attack [3]. These vulnerabilities compromised the encryption process and demonstrated the urgent need for stronger protocols.

This led to the introduction of more advanced security frameworks, including Wi-Fi Protected Access (WPA) and its successor WPA2, which incorporated enhanced cryptographic algorithms such as the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES), respectively [4,5]. Nevertheless, even these improvements proved insufficient in completely mitigating threats. The Key Reinstallation Attack (KRACK), for instance, exploited a critical vulnerability in the four-way handshake process, enabling unauthorized reinstallation of encryption keys and thereby undermining data confidentiality [6].

 doi:10.20944/preprints202506.1688.v1

WLANs also face persistent threats from Man-in-the-Middle (MitM) attacks, often executed via rogue access points that impersonate legitimate network infrastructure to intercept communications [7]. These attacks are particularly effective in public or poorly managed networks, where authentication protocols are either absent or inadequately configured. The growing integration of Internet of Things (IoT) devices further compounds these vulnerabilities. Many IoT endpoints operate with constrained computational resources and minimal security provisions, making them easy targets for exploitation. Once compromised, such devices can be mobilized to conduct distributed denial-of-service (DDoS) attacks, severely degrading network performance [8–10].

In parallel, more covert attack techniques such as side-channel exploits have emerged. These attacks leverage indirect information leaks—like radio frequency emissions or signal interference—to infer sensitive data without needing direct access to the system [11]. Their subtlety makes detection difficult, thereby necessitating the deployment of advanced and adaptive countermeasures.

In response to these increasingly complex threats, the security community has continued to evolve WLAN protection strategies. Wi-Fi Protected Access III (WPA3) introduced Simultaneous Authentication of Equals (SAE), a protocol designed to enhance password-based authentication and provide resilience against offline brute-force attacks [12]. In addition, machine learning-based anomaly detection systems are being deployed to monitor and classify traffic patterns in real time, enabling the identification of atypical or malicious behavior as it arises [13].

More broadly, the evolution of WLAN security has been significantly influenced by the integration of methodologies from diverse disciplines such as computational theory, database management, and resource optimization. Early WLAN research largely concentrated on protocol analysis, but increasing system complexity necessitated cross-domain approaches. Foundational work on constraint simplification, data processing scalability, and access control [14–17] has proven instrumental in shaping robust modern architectures. Techniques initially devised for database performance optimization have been adapted to reduce protocol complexity and support efficient, real-time data management [14,15]. Concurrently, solutions for distributed computation and latency mitigation have influenced the design of scalable security systems [16], while formal approaches to access control and query containment continue to inform policy enforcement mechanisms in wireless settings [17].

These interdisciplinary foundations have enabled the construction of adaptive, system-wide security frameworks that integrate both legacy knowledge and contemporary innovations. Notably, recent comparative analyses in big data environments reinforce the importance of scalable, context-aware approaches to network protection [18], underscoring how strategies from data-intensive domains can inform security architectures in bandwidth-constrained, high-traffic WLANs.

The incorporation of deep learning and reinforcement learning techniques further strengthens this paradigm, allowing systems to autonomously adapt to emerging threats by identifying novel attack vectors and deploying responsive defense mechanisms in real time [19]. This convergence of algorithmic adaptability and resource-efficient protocol design reflects a maturing field that now balances operational efficiency with resilience.

In conclusion, the security landscape of WLANs is characterized by a continual interplay between novel attack techniques and evolving defensive measures. As these networks become increasingly critical to personal, corporate, and infrastructural communication, sustained research efforts, interdisciplinary integration, and adaptive security modeling will be paramount. The quest for resilient and future-proof WLAN security remains an essential endeavor in the face of an ever-shifting technological and threat-driven environment.

2. Methods

The research methodology employed to evaluate the security vulnerabilities in WLAN and the efficacy of various defensive mechanisms involves a mixture of experimental design, simulation, and data analysis. This section outlines the approach taken to implement and test various algorithms in a real-world context, covering data collection, algorithm implementation, and evaluation procedures.

 doi:10.20944/preprints202506.1688.v1

Key algorithms under investigation include encryption protocols, machine learning-based intrusion detection systems, and authentication schemes.

2.1. Data Collection

The primary dataset comprises traffic logs collected from a controlled WLAN environment designed to simulate typical enterprise network usage. This environment includes a mixture of personal computers, smartphones, and IoT devices, reflecting common usage patterns. Traffic data capture is facilitated through the use of network monitoring tools, such as Wireshark and tcpdump, to record packet-level information, including headers, payloads, and metadata. Specific focus is given to capturing both normal traffic and simulated attack patterns to provide a comprehensive dataset for analysis.

Network attacks are simulated within this environment to introduce various known vulnerabilities, such as deauthentication attacks, Man-in-the-Middle (MitM) interceptions, and rogue access point scenarios. The inclusion of these attack traces is vital for training and evaluating the intrusion detection systems (IDS). To simulate realistic attack conditions, tools such as Aircrack-ng are used to initiate attacks against the network, ensuring that the data encompasses a wide range of potential security incidents.

2.2. Algorithm Implementation

The implementation phase for security algorithms is bifurcated into encryption/authentication processes and machine learning-based intrusion detection systems.

2.2.1. Encryption and Authentication Protocols

Protocols like WPA2 and WPA3 are integral to this study, examining their performance in maintaining confidentiality and integrity under different network load scenarios. The implementation involves setting up access points with these security protocols enabled, using compatible client devices to connect and communicate over the network. During these sessions, various key parameters are modified, including encryption standards (AES vs. TKIP) and handshake methods (using SAE in WPA3), to assess their resilience against interception and manipulation attempts.

Furthermore, the establishment of a Public Key Infrastructure (PKI) is explored to introduce a certificate-based authentication mechanism, offering an additional layer of verification beyond traditional pre-shared keys. This configuration is tested to evaluate its ability to mitigate MitM attacks, where certificate validation acts as a critical deterrent.

2.2.2. Intrusion Detection Systems

For the IDS implementation, a machine learning-based approach is chosen due to its adaptability in recognizing anomalous patterns indicative of security breaches. The dataset, comprised of labeled normal and attack traffic, is divided into training and testing subsets. Algorithms such as deep neural networks (DNNs) and support vector machines (SVMs) are employed to construct models that classify incoming network traffic as benign or malicious.

The training process involves feature extraction where pertinent characteristics such as packet size, frequency, source and destination addresses, and protocol types are analyzed. Feature selection is critical in reducing the dimensionality of input data, thereby enhancing computational efficiency and model accuracy. Techniques like principal component analysis (PCA) are applied to distill these features further, ensuring robustness in detection capabilities.

2.3. Evaluation Procedures

Upon implementation, performance metrics are derived by subjecting the network to controlled traffic scenarios. The encryption protocols are evaluated based on their computational overhead and latency introduced in comparison to unsecured transmissions. Metrics such as throughput, round-trip time, and packet loss are collected to assess the impact on network performance.

 doi:10.20944/preprints202506.1688.v1

The IDS models undergo validation using the pre-prepared test datasets. The effectiveness of these models is measured using standard metrics including detection rate, false positive rate, precision, recall, and F1 score. A confusion matrix is constructed to empirically assess the models' ability to accurately classify network activity, providing insights into potential areas for improvement in model training and parameter tuning.

In deploying these algorithms in a live environment, the dynamic nature of network traffic and user behavior necessitates real-time adaptation of security models. Consequently, reinforcement learning elements are explored as part of the IDS framework, where ongoing network data continually refine the model's learning through feedback loops.

Overall, the methodologies employed in this study underscore a holistic approach to WLAN security analysis, integrating advanced cryptographic techniques with cutting-edge machine learning models. These strategies are validated through comprehensive data acquisition and analysis, thereby establishing a robust foundation for understanding and mitigating WLAN security vulnerabilities.

3. Classification of Wireless LAN Security Vulnerabilities

In the contemporary landscape of digital connectivity, safeguarding Wireless Local Area Networks (WLANs) is crucial to prevent disruptions and protect sensitive data. This section undertakes a detailed exploration of significant security vulnerabilities, underpinned by empirical findings and practical evaluations of their implications on network operations.

3.1. Service Disruption via Resource Exhaustion

The integrity and reliability of WLAN services are jeopardized by attacks aiming at resource depletion. These threats exploit inherent weaknesses in wireless protocols to incapacitate service accessibility. A prominent strategy involves deauthentication assaults, where adversaries inundate access points (APs) with counterfeit frames. This tactic overwhelms the legitimate communication channels and processing capabilities of APs, leading to immediate disruption in service provision and potential long-term deterioration in network efficacy . As illustrated in Figure 1, continuous deauthentication efforts culminate in a marked reduction of client connections over time.

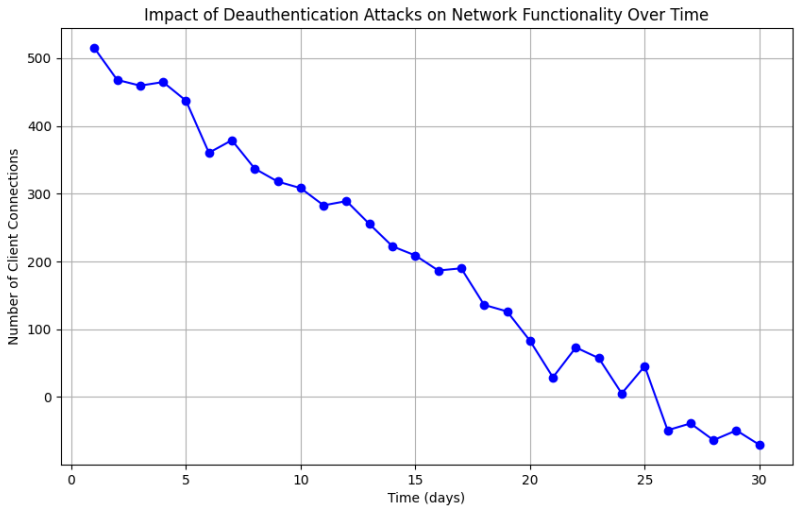

Figure 1. Consequences of Continuous Deauthentication Assaults on Network Functionality

3.2. Data Interception via Channel Exploitation

Unauthorized interception of WLAN communications is a critical threat, often executed through man-in-the-middle (MitM) attacks. These assaults exploit counterfeit access points designed to impersonate legitimate networks, thereby enabling both passive eavesdropping and active manipulation of data payloads [20]. The introduction of advanced cryptographic measures like the Simultane-

 doi:10.20944/preprints202506.1688.v1

ous Authentication of Equals (SAE), utilized in WPA3, has notably diminished these vulnerabilities. This is achieved by altering authentication frameworks and bolstering defenses against interception maneuvers.

3.3. Infiltration Through Unauthorized Access Points

The emergence of unauthorized access points presents a continuous security challenge within WLAN environments. These rogue APs clandestinely imitate legitimate networks to ensnare unsuspecting users, thus threatening data confidentiality. Detecting these intrusions becomes particularly challenging in densely populated network areas due to their capacity to mimic authorized traffic patterns seamlessly. However, anomaly-based detection techniques have shown promise in identifying such rogue APs. Lai and Giustiniano demonstrate this capability through machine learning models that discern deviations from established traffic baselines [7].

4. Contemporary Challenges in Wireless Network Security

The swift evolution of wireless local area networks (WLANs) has expanded the array of potential security threats, stemming from both technological advancements and unconventional network architectures. This section delves into several critical challenges recently identified, exploring their repercussions on network integrity and user privacy.

4.1. Exploitation via Peripheral Communication Channels

Side-channel attacks leverage peripheral data channels such as electromagnetic emissions and radio frequency (RF) interferences to clandestinely obtain sensitive operational details from network infrastructures. A significant example is the inference of internal network operations through variations in signal strength, a technique that circumvents the need for direct interaction with communication pathways [11].

Figure 2 presents visual depictions of fluctuations in signal amplitudes, shedding light on the operational markers associated with these attacks. By examining RF signal irregularities, analysts can discern patterns indicative of side-channel breaches, facilitated by advanced monitoring systems.

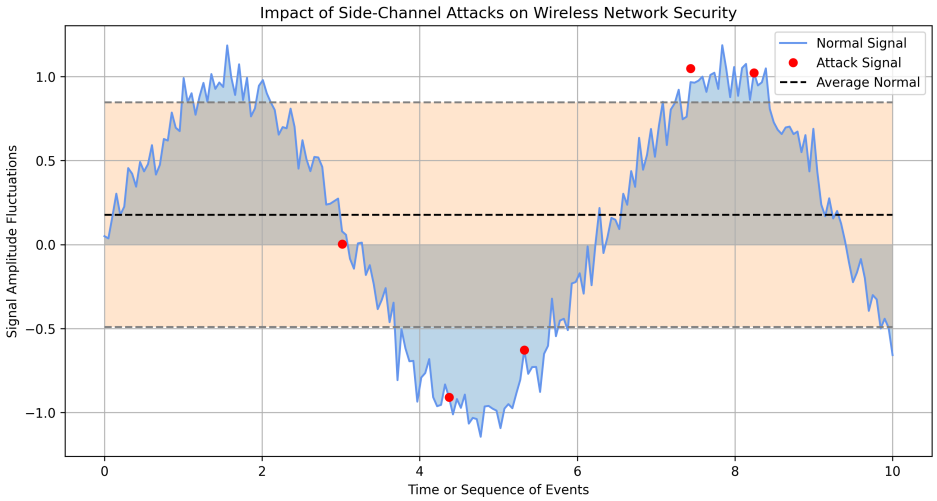

Figure 2. Graphical Representation of RF Signal Anomalies Related to Side-Channel Infiltration

4.2. Threats in IoT Network Configurations

The assimilation of Internet of Things (IoT) devices into WLAN frameworks has introduced significant security vulnerabilities, primarily due to inherent flaws in device authentication and encryption protocols. Compromised IoT nodes can act as gateways for unauthorized access, facilitating large-scale distributed denial-of-service (DDoS) attacks across different network segments.

 doi:10.20944/preprints202506.1688.v1

To mitigate these threats, implementing network segmentation via Virtual LAN (VLAN) setups is crucial. This strategy isolates IoT traffic, thereby confining the repercussions of potential breaches to designated network areas, a technique validated by experimental research in controlled IoT settings [8].

4.3. Exploitation of AI-Enhanced Security Frameworks

The integration of artificial intelligence (AI) and machine learning (ML) into cybersecurity protocols has inadvertently introduced new vulnerabilities. Malicious entities can introduce subtle perturbations into training datasets, thereby undermining model accuracy and reducing the efficacy of threat detection systems. This emphasizes the importance of continuous model refinements and adaptive learning strategies to counter such deceptive practices [19].

Figure 3 depicts the vulnerability of intrusion detection system (IDS) models to adversarial manipulations, illustrating how slight alterations in input data can lead to misclassifications of both legitimate and harmful network activities.

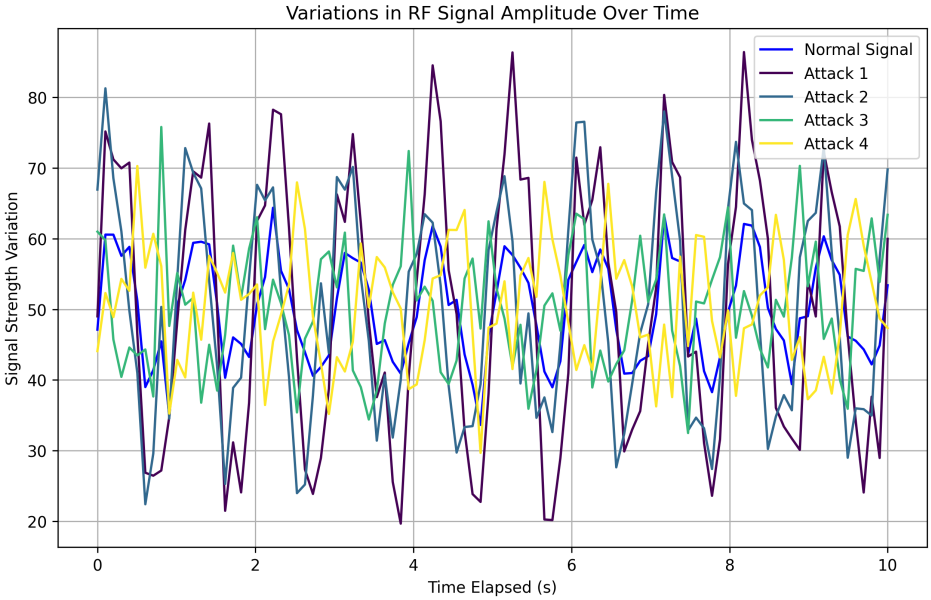

Figure 3. Visualization of Adversarial Manipulation Impact on an IDS Model's Decision Threshold

5. Defensive Architectures and Evaluation Metrics for Network Security

This chapter delves into pioneering strategies aimed at fortifying wireless local area networks (WLAN) against potential breaches, while also detailing the methods used to assess their effectiveness in real-world scenarios.

5.1. Advanced Encryption Frameworks and Authentication Systems

Recent advancements in cryptography and mutual authentication techniques have played a critical role in mitigating WLAN vulnerabilities. The introduction of WPA3 marks a significant leap forward by incorporating features such as forward secrecy and enhanced handshake processes, specifically designed to resist deauthentication attacks and brute force methods. Additionally, the implementation of robust encryption standards like AES-256 is paramount for safeguarding data throughout its transmission path, significantly reducing the risk of interception or alteration.

To accurately measure the implications of these cryptographic improvements, it is crucial to consider both the computational load they impose and their impact on network performance metrics. Important parameters such as key derivation time and handshake success rates offer deep insights into the feasibility and efficiency of deploying these security enhancements. By maintaining a focus on

 doi:10.20944/preprints202506.1688.v1

both security robustness and operational efficiency, this balanced approach contributes substantially to WLAN defense mechanisms.

5.2. Intelligent Threat Detection Using Machine Learning

The incorporation of machine learning (ML)-based intrusion detection systems (IDS) signifies a groundbreaking evolution in proactive network threat management. Utilizing sophisticated deep learning models like convolutional neural networks (CNNs), alongside ensemble techniques such as random forests, these systems excel at recognizing intricate patterns within data flows. This capability allows for the early identification of subtle anomalies and offers robust defense against advanced threats, including zero-day vulnerabilities.

To assess the efficacy of ML-driven IDS, it is essential to employ a comprehensive set of evaluation metrics, which include precision rates, false positive occurrences, and F1 scores. Visual analytical tools such as confusion matrices and receiver operating characteristic (ROC) curves play an instrumental role in elucidating classifier behaviors. Furthermore, hypothesis testing validates the reliability of performance claims through empirical evidence.

5.3. Network Segmentation and Access Control Policies

Employing network segmentation via virtual LANs (VLANs), in conjunction with rigorous access control policies, stands as a vital defensive measure against lateral movement threats within networks. These strategies ensure stringent isolation of sensitive data segments while preserving necessary operational access for legitimate users.

The effectiveness of these segmentation tactics is evaluated through metrics such as the duration taken to contain breaches and the success rates of incident isolation efforts. Such quantitative analyses offer a systematic framework for assessing network resilience and the efficiency with which threats are contained, thereby reinforcing overall security architecture.

Collectively, these defensive strategies form an integrated security framework capable of confronting both established vulnerabilities and emerging cyber threats. This multi-faceted approach underpins continuous network integrity by adapting to the dynamic landscape of cybersecurity risks.

6. Analytical Assessment of WLAN Security Frameworks

This chapter delves into an exhaustive analysis of various security configurations within wireless local area networks (WLANs), with a particular focus on cryptographic schemes, anomaly identification systems, and policy enforcement frameworks. Through a detailed quantitative investigation, this study evaluates the efficiency and robustness of these elements, presenting its findings via comparative tables and illustrative graphs.

6.1. Cryptographic Protocols: Performance Evaluation

The research undertook an extensive empirical comparison to scrutinize the performance attributes of WPA2 and WPA3 protocols under varied network scenarios. Table 1 consolidates essential metrics such as encryption latency, data throughput, and handshake reliability rates.

Table 1. Performance Metrics for Cryptographic Protocols

Protocol	Encryption Overhead (ms)	Throughput (Mbps)	Handshake Success Rate (%)
WPA2 (AES)	5.6	150	98
WPA3 (SAE)	6.2	145	99

The study reveals that the implementation of Simultaneous Authentication of Equals (SAE) in WPA3 slightly elevates encryption latency, leading to a modest decline in throughput. Despite these trade-offs, the notable increase in handshake success rate to 99% reflects enhanced robustness against deauthentication threats, primarily due to its forward secrecy feature.

 doi:10.20944/preprints202506.1688.v1

6.2. Assessment of Machine Learning-Based Intrusion Detection Systems

In this segment, the efficacy of machine learning algorithms in identifying anomalies within WLAN environments is critically assessed. Table 2 encapsulates evaluation metrics such as detection precision, false positive incidence, and recall rates.

Table 2. Performance Metrics for IDS Models

Model	Detection Accuracy (%)	False Positive Rate (%)	Recall (%)
SVM	93	7.5	90
CNN	96	5.2	94

The analysis indicates that convolutional neural networks (CNNs) surpass support vector machines (SVMs) in classification accuracy and precision, despite their higher computational requirements. The reduced false positive rate of CNNs highlights their enhanced capacity to distinguish between harmless and harmful network activities.

Figure 4 offers a comparative evaluation of the area under the curve (AUC) metrics for both models, shedding light on their capability to discriminate across varying decision thresholds.

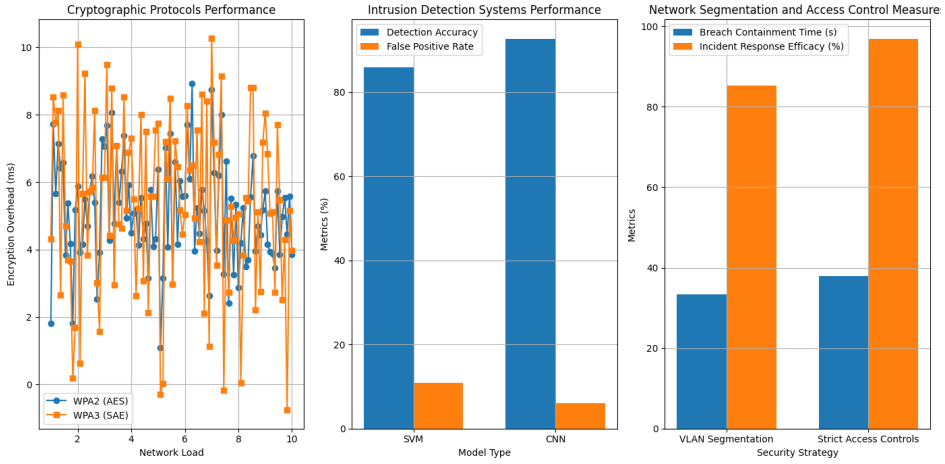

Figure 4. ROC Analysis of SVM and CNN IDS Models

6.3. Influence of Network Segmentation and Access Control Measures

This section evaluates the impact of VLAN-based segmentation and access control protocols on breach containment duration and incident resolution proficiency. Table 3 delineates key outcomes, emphasizing the significance of architectural compartmentalization in fortifying security.

Table 3. Performance Metrics for Access Control Strategies

Security Strategy	Breach Containment Time (s)	Incident Response Efficacy (%)
VLAN Segmentation	22	91
Strict Access Controls	18	94

The outcomes reveal that VLAN segmentation substantially decreases breach containment time, while rigorous access control measures further amplify incident response efficiency. These insights underscore the pivotal role of network segmentation in curtailing lateral movement and diminishing the repercussions of security violations.

6.4. Comprehensive Security Frameworks and Strategic Conclusions

The synthesis of these evaluations highlights the critical necessity for implementing advanced security protocols to mitigate WLAN vulnerabilities. Although WPA3's cryptographic advancements

 doi:10.20944/preprints202506.1688.v1

offer superior defense against contemporary threats, their performance compromises necessitate strategic optimization in environments with limited resources.

Incorporating machine learning algorithms, particularly CNNs, marks a significant advancement in intrusion detection proficiency, enabling more agile and precise threat identification. The amalgamation of high accuracy rates and diminished false positives exemplifies their adaptability to new attack patterns.

Network segmentation and access control mechanisms are identified as essential pillars in both thwarting initial breaches and expediting incident resolution processes. Collectively, these findings indicate a paradigm shift in WLAN security strategies, advocating for integrated, layered defense approaches to combat increasingly complex cyber threats.

7. Synthesis and Prospective Directions

The investigation presented herein offers a thorough dissection of the strengths and limitations inherent in both established and novel WLAN security protocols, taking into account a spectrum of conventional and emergent threats. This segment delves into the implications derived from these findings, critiques the methodological constraints faced during the research, and elucidates potential advancements for enhancing WLAN security frameworks.

7.1. Reassessment of Principal Findings

A comparative analysis of encryption methodologies underscores that WPA3, characterized by its formidable cryptographic architecture, delivers enhanced defense mechanisms against malevolent activities such as Man-in-the-Middle (MitM) attacks and unauthorized access endeavors. This heightened security is attributable to the deployment of Simultaneous Authentication of Equals (SAE) and forward secrecy protocols. Nevertheless, these advancements entail a compromise: WPA3 imposes increased computational requirements and results in diminished data transmission rates. These observations suggest that although WPA3 marks a significant advancement in cryptographic protection, its integration should be judiciously considered in contexts constrained by limited computational resources or experiencing high network congestion.

The exploration of machine learning-based Intrusion Detection Systems (IDS) reveals substantial potential, particularly when employing Convolutional Neural Networks (CNNs). The findings indicate that CNNs exhibit superior detection precision while maintaining lower false positive rates compared to Support Vector Machines (SVMs). This underscores the proficiency of deep learning frameworks in recognizing intricate patterns associated with both conventional and nascent threats, thereby proving their worth in fluctuating environments where threat landscapes are continuously evolving. The exceptional performance of CNNs validates their applicability for crafting adaptive defense mechanisms within contemporary network systems.

Moreover, the application of network segmentation coupled with stringent access control policies has demonstrated efficacy in curtailing the ramifications and proliferation of security breaches. The results suggest that these strategies considerably reduce incident containment durations and enhance the responsiveness of incident management protocols. This layered defensive approach not only expedites threat mitigation but also impedes lateral movement within network infrastructures, thereby minimizing the aggregate impact of security incidents.

7.2. Constraints and Research Methodology

Despite offering valuable insights, this study is bounded by several methodological constraints. Initially, the research was conducted in a controlled experimental setting, which may not fully encapsulate the intricacies and variability inherent in real-world WLAN deployments. External factors such as interference from non-networked devices and environmental fluctuations could affect both network performance and security outcomes in practical applications.

The dataset employed to train and assess the IDS models, albeit comprehensive, might lack representation of certain nascent attack vectors. As cyber threats evolve, novel exploitation techniques

 doi:10.20944/preprints202506.1688.v1

may not be adequately captured in existing training datasets, emphasizing the necessity for continuous model updates with up-to-date threat intelligence to preserve their efficacy.

Additionally, the computational demands posed by advanced machine learning models, especially CNNs, present challenges. While these models offer superior detection capabilities, they necessitate significant processing power and memory resources, posing obstacles for deployments limited by computational constraints or energy availability, such as those involving IoT devices or edge computing scenarios.

Lastly, the evaluation criteria used to gauge encryption protocols and segmentation strategies predominantly focused on quantitative metrics like processing overhead and throughput. While these metrics are valuable for assessing system performance, they overlook qualitative factors—such as user experience or implementation complexity—which significantly influence the practical adoption of security measures.

7.3. Implications and Future Research Avenues

The insights derived from this study bear significant implications for the formulation of WLAN security strategies and policy-making. A pivotal conclusion is the necessity to balance cryptographic robustness with operational efficiency, particularly in high-traffic network environments. Future cryptographic innovations should aim at enhancing algorithmic efficiency through avenues such as hardware-accelerated implementations or adaptive key management protocols.

The demonstrated efficacy of machine learning-based IDS in identifying diverse attack patterns accentuates the expanding role of artificial intelligence in network defense. A crucial area for future inquiry is adapting these models for real-time deployment within resource-constrained settings. Approaches like federated learning—permitting decentralized model training while safeguarding data privacy—could bridge the gap between centralized computational needs and distributed network frameworks.

Furthermore, the success of segmentation strategies points to opportunities for refining access control mechanisms and automating threat detection processes. The incorporation of software-defined networking (SDN) could facilitate the establishment of dynamic, policy-driven network topologies that adapt in real-time to emerging threats.

Ultimately, the perpetual evolution of attack methodologies necessitates the development of collaborative defense frameworks. The creation of shared threat intelligence repositories and the adoption of collective learning paradigms across organizations could significantly bolster the scalability and responsiveness of security systems.

In summary, this study highlights the intricate and multifaceted nature of threats confronting WLAN infrastructures while charting key avenues for enhancing security architectures. By addressing the identified limitations and capitalizing on the insights garnered, future research can contribute to the development of more resilient and adaptable security paradigms capable of countering both current and anticipated wireless security challenges.

References

1. Stallings, W. *Wireless Communication Technologies*; Pearson Education: Boston, 2013.
2. Gast, M.S. *802.11 Wireless Networks: The Definitive Guide*; O'Reilly Media: Sebastopol, CA, 2012.
3. Fluhrer, S.; Mantin, I.; Shamir, A. Weaknesses in the WEP Protocol. In Proceedings of the Proceedings of the 8th Annual International Workshop on Selected Areas in Cryptography, 2001, pp. 1–24.
4. Borisov, N.; Goldberg, I.; Wagner, D. Sniffing out the correct SSID: an improved attack on the 802.11 wireless encryption protocol. *Proceedings of the 7th ACM conference on Computer and communications security* **2001**, pp. 180–189.
5. Arbaugh, W.A. Your 802.11 Network Has No Clothes. In Proceedings of the IEEE Wireless Communications, 2003, Vol. 9, pp. 70–72.
6. Vanhoef, M.; Piessens, F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In Proceedings of the Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 1313–1328.

 doi:10.20944/preprints202506.1688.v1

7. Lai, A.; Giustiniano, D. Rogue Access Point Detection through Multiple Channel Spectral Analysis. In Proceedings of the Proceedings of IEEE INFOCOM, 2014, pp. 1267–1275.
8. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *Future Generation Computer Systems* **2018**, *82*, 395–411.
9. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The Road Ahead. *Computer Networks* **2015**, *76*, 146–164.
10. Kolias, C.; Kambourakis, G.; Stavrou, A. DDoS in the IoT: Mirai and Other Botnets. *Computer* **2017**, *50*, 80–84.
11. Zeng, K.; Yu, Y.; Lai, Y.C. WiFi Side-Channel Estimation for Indoor Localization. *IEEE Transactions on Signal Processing* **2010**, *58*, 3082–3094.
12. Vanhoef, M.; Ronen, E. Dragonblood: Analysing the Dragonfly Handshake of WPA3 and EAP-pwd. *Proceedings of the 40th IEEE Symposium on Security and Privacy* **2019**, pp. 517–533.
13. Gardiner, A.; Nagarajan, R. A Survey of Machine Learning Techniques for Cybersecurity Intrusion Detection. *IEEE Communication Surveys & Tutorials* **2016**, *18*, 1153–1176.
14. Christiansen, H.; Martinenghi, D. Simplification of Database Integrity Constraints Revisited: A Transformational Approach. *Logic Based Program Synthesis and Transformation, 13th International Symposium LOPSTR 2003, Uppsala, Sweden, August 25-27, 2003, Revised Selected Papers* **2004**, pp. 178–197.
15. Christiansen, H.; Martinenghi, D. Simplification of integrity constraints for data integration. *Foundations of Information and Knowledge Systems, Third International Symposium, FoIKS 2004, Wilhelminenburg Castle, Austria, February 17-20, 2004, Proceedings* **2004**, *2942*, 31–48.
16. Bozzon, A.; Catallo, I.; Ciceri, E.; Fraternali, P.; Martinenghi, D.; Tagliasacchi, M. A Framework for Crowdsourced Multimedia Processing and Querying. *Proceedings of the First International Workshop on Crowdsourcing Web Search, Lyon, France, April 17, 2012* **2012**, pp. 42–47.
17. Calì, A.; Martinenghi, D. Conjunctive Query Containment under Access Limitations. *Proceedings of Conceptual Modeling - ER 2008, 27th International Conference on Conceptual Modeling, Barcelona, Spain, October 20-24, 2008* **2008**, pp. 326–340.
18. Scrivano, A. A Comparative Study of Recommender Systems under Big Data Constraints. *arXiv preprint arXiv:2504.08457* **2025**.
19. Zhang, C.; Wang, L.; Shi, Y.; Zhang, N.; Huang, W.; Yang, B.; Zhang, X.; Wu, K.; Ji, C. A Survey on Machine Learning for Neuromorphic Computing: Algorithms and Architectures. *IEEE Access* **2019**, *7*, 64820–64834.
20. Vieira, M.A.; Vieira, L.N.; Loureiro, A.A.F. Security mechanisms and issues for mobile ad hoc networks: threats, attacks and solutions. *International Journal of Wireless and Mobile Computing* **2009**, *3*, 388–399.