Wireless Wi-Fi Access Point Security: An Analysis of WPA, WPA2, WPS, and WPA3.

Vidhan Dilip Gambhire[1], Sushant Ramchandra Gade[2], Sandhya Kaprawan[3], Aniket Gupta[4]
[1,2,3,4]*University Department of Information & Technology (MSC. Cybersecurity), University of Mumbai.*

***Abstract*—Wireless Local Area Networks (WLANs) are the pillars of both household and business networking, breaking barriers in wireless connectivity, but rather they still are susceptible to attacks than ever. Recent security protocols have introduced enhancements such as improved encryption and authentication mechanisms, yet they are inadequate solutions to the availability-oriented attacks such as deauthentication floods, denial-of-service (DoS), and distributed denial-of-service (DDoS) attacks. On another side, the paper contains an organized comparison of WPA, WPS, and WPA3, including the areas in which they have improved and the persistent problems in actual use.**

The OpenWRT-based router-level security framework that the current study suggests is a tool to close the identified gaps. This framework enables the router to actively monitor and mitigate malicious traffic. The proposed way is based on real-time traffic observation, anomaly detection according to traffic patterns, and dynamic firewall rules enforcement to deny access to malicious entities at the router itself. Both theoretical explanation and practical experiment show that a normal Wi-Fi router can be an active-security hardware only if it has certain security features, therefore, the network's resilience is better. The computations indicate that security on the application protocol level is able to stand it well only if complementary measures of router level are taken into account.

I. INTRODUCTION:

WLANs form one of the basic building blocks of digital infrastructure today, supporting applications running from residential to commercial and institutional settings. From personal communications and cloud access to IoT deployments and business operations, Wi-Fi connectivity has become intricately embedded into daily computing. As reliance on wireless networks continued to expand, so did the attack surface, making Wi-Fi security one of the linchpins within modern cybersecurity research.Historically, Wi-Fi security mechanisms have evolved from early standards such as WEP to robust protocols including WPA, WPA2, and the recently introduced WPA3. Every new generation tries to address deficiencies of the previous generations by improving encryption, enhancing authentication processes, and reducing vulnerability to common attacks. While WPA3 introduces some enhancements, like SAE (Simultaneous Authentication of Equals) and enhanced resistance to offline dictionary attacks, practical security challenges remain in real-world deployments of Wi-Fi. In particular, availability-oriented attacks like deauthentication floods, denial-of-service (DoS), and DDoS events remain only partially mitigated by protocol-level security measures.

A large part of the current Wi-Fi security solutions focuses on confidentiality and authentication, often considering the access point as a passive forwarding device. Therefore, most routers cannot actively detect and respond to abnormal traffic patterns that compromise network availability. This is particularly critical in the home and small enterprise contexts, where sophisticated external intrusion detection systems are seldom deployed due to the cost and complexity. Thus, there is an emerging need for mechanisms at the access point that are able to provide real-time security defenses.

This work critically analyzes, both from theoretical and practical perspectives, the security limitations of WPA, WPA2, WPS, and WPA3 with respect to availability threats. Grounded on the foregoing analysis, the paper proposes an OpenWRT-based router-level security framework able to perform active traffic monitoring and dynamic mitigation of malicious activity. The approach proposed here rearranges the Wi-Fi access point from a passive network bridge to an active security component by

leveraging packet-level observation, logging, and firewall enforcement directly at the router. The objective of this research is not to redefine cryptographic protocols but to illustrate the fact that good Wi-Fi security requires a multilayered approach whereby protocol-level defenses must be augmented by real-time, router-level mechanisms. By means of analytical evaluation and empirical experimentation, the work will demonstrate how open-source router platforms like OpenWRT can be leveraged to improve the resilience of wireless networks against current and future cyber threats in residential and business environments.

II. BACKGROUND OF WIRELESS NETWORK SECURITY:

Wireless network security is conventionally achieved through cryptographic protocols at multiple layers in the network stack, including IPSecurity, Wi-Fi Protected Access, and Secure Sockets Layer [7]. These traditional approaches, while fundamental, are increasingly challenged by the evolving threat landscape, particularly with the advent of next-generation wireless systems like 5G, 6G, and Wi-Fi 7/8, which introduce advanced features and expanded attack surfaces [3] [8]. For instance, the inherent vulnerabilities of open Wi-Fi networks to man-in-the-middle attacks highlight the continuous need for enhanced confidentiality measures, such as those provided by Wi-Fi Protected Access 3 [3] [9]. However, the proliferation of sophisticated cyber threats, including advanced persistent threats and zero-day exploits, mandates the integration of advanced security solutions such as post-quantum cryptography, multi-factor authentication, and AI-based intrusion detection systems [3].

Moreover, the open nature of wireless transmission inherently exposes networks to vulnerabilities such as eavesdropping, denial-of-service attacks, spoofing, man-in-the-middle attacks, and message falsification, demanding robust cryptographic techniques and vigilant monitoring to ensure data integrity and user authenticity [10] [3].

III. OVERVIEW OF WI-FI SECURITY PROTOCOLS:

The evolution of Wi-Fi security protocols reflects a continuous arms race between security developers and malicious actors, starting with early, vulnerable standards and progressing towards more resilient cryptographic mechanisms [12]. This section will detail the progression from Wired Equivalent Privacy to Wi-Fi Protected Access (WPA, WPA2, and WPA3), analyzing the cryptographic foundations, inherent weaknesses, and subsequent improvements introduced with each iteration. Specifically, it will examine WEP's reliance on the RC4 stream cipher and static pre-shared keys, which quickly proved insufficient against common attacks, and then explore the subsequent development of WPA and WPA2, highlighting their enhanced encryption and authentication mechanisms.

The discussion will then transition to the significant advancements introduced with WPA3, which addresses the inherent vulnerabilities of previous protocols by implementing more robust cryptographic algorithms and enhanced authentication protocols, thereby mitigating risks such as dictionary attacks and ensuring forward secrecy. This progression underscores the critical importance of understanding each protocol's strengths and weaknesses to implement effective security strategies in diverse Wi-Fi environments [13]. Furthermore, a comprehensive understanding of Wi-Fi Protected Setup is crucial, given its widespread adoption and documented security flaws that can expose networks to brute-force attacks, thereby undermining the stronger protections offered by WPA2 and WPA3.

The ongoing development of Wi-Fi standards, such as Wi-Fi 6E and the impending Wi-Fi 7, further complicates the security landscape by introducing new frequency bands, increased throughput, and advanced modulation schemes that require reassessment of existing security paradigms to ensure continued protection against evolving threats. This paper will therefore analyze the security protocols WPA, WPA2, WPS, and WPA3, assessing their effectiveness in safeguarding wireless networks against common cyber threats, with a particular focus on their application in home and commercial settings [14].

IV. LITERATURE REVIEW:

The article methodically covers a wide range of wireless network security topics, with an emphasis on the evolution of Wi-Fi protocols from WEP to the most recent WPA3, as well as the theoretical vulnerabilities associated with each standard. These settings highlight the discrepancy between the real-world security model and its theoretical counterpart. Many of those gaps were filled by WPA2, which made the use of AES encryption and other security improvements for enterprise authentication necessary. WPA2 still has a lot of flaws, though, particularly when it comes to PMKID assaults and the potential for a downgrade attack in a mixed-mode deployment scenario.

Moreover, the pervasive nature of wireless network traffic makes it a prime target for various attacks, highlighting the critical need for robust, automated detection and blocking mechanisms that go beyond passive security protocols [22]. This imperative for advanced cybersecurity solutions has led to the development of sophisticated intrusion detection systems that scrutinize network traffic for anomalies and potential threats, issuing alerts upon detection [23]. However, such systems often operate at the perimeter or within the network, frequently lacking the capability for direct, router-level intervention to block malicious MAC addresses in real-time, especially in the context of DoS and DDoS attacks [24].

This limitation underscores the necessity for developing predictive modeling techniques and advanced anomaly detection mechanisms that can discern between normal fluctuations and malicious activities, such as spoofed data or coordinated attacks [25]. Such systems must also contend with the limitations of conventional MAC address identification, as many IoT devices randomize their MACs, making it difficult to differentiate legitimate traffic from spoofing attempts [26] [27]. Therefore, advanced MAC association frameworks are crucial to track devices despite randomization, enabling more reliable threat identification and mitigation in dynamic environments [27]. However, challenges remain in real-time data processing, particularly in handling the immense volume of wireless traffic for immediate threat identification [3]. The complexity of distinguishing legitimate traffic from malicious activity, such as sophisticated man-in-the-middle or injection attacks, further complicates the development of effective, unified protection methods [15].

This evolving landscape of threats necessitates a comprehensive approach that integrates advanced machine learning models with real-time adaptive defense mechanisms to predict and counteract sophisticated attacks [25]. Such a framework would move beyond mere detection by actively blocking identified malicious entities, thereby preventing their continued access and safeguarding network integrity [25]

V. EVOLUTION OF WI-FI SECURITY STANDARDS:

The progression of Wi-Fi security protocols, from the initial Wired Equivalent Privacy to the current Wi-Fi Protected Access 3, reflects a continuous effort to fortify wireless networks against an increasingly sophisticated array of cyber threats. Initially, WEP offered basic encryption, yet its fundamental flaws, particularly its weak initialization vector, rendered it highly vulnerable to attacks [10]. This led to its rapid deprecation in favor of WPA, which introduced Temporal Key Integrity Protocol for dynamic key management and message integrity checks, significantly improving upon WEP's cryptographic weaknesses. However, WPA still utilized the RC4 stream cipher, inheriting some of its vulnerabilities and prompting the development of WPA2 [10]. WPA2 subsequently implemented the stronger Advanced Encryption Standard along with the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol to provide more robust data confidentiality and integrity. Despite these advancements, WPA2's enterprise mode introduced its own set of management complexities, particularly concerning key distribution and certificate validation within larger networks [10]. This complexity often leads to misconfigurations that can expose networks to vulnerabilities, such as rogue access points or insider threats.

VI. ANALYSIS OF WPA AND WPA2 VULNERABILITIES:

While WPA and WPA2 offered substantial improvements over WEP, they are not without their weaknesses, which have been extensively documented and exploited in various attack vectors. For instance,

WPA is notably vulnerable to dictionary attacks when relying on weak pre-shared keys, while WPA2 has exhibited susceptibility to key reinstallation attacks that compromise data confidentiality [10] [28].

The discovery of the KRACK against WPA2 highlighted fundamental weaknesses in the four-way handshake, enabling attackers to reinstall an already-in-use key, which can lead to decryption of frames, packet injection, and other critical security breaches [29].

Further research has also shown that even WPA-Enterprise systems, including widely deployed networks like Eduroam, exhibit a significant lack of user awareness regarding documented vulnerabilities, leading to successful Man-in-the-Middle and Denial of Service attacks despite existing literature detailing such threats [14].

These vulnerabilities are not inherent to the 802.1X mechanisms themselves, but rather stem from misconfigurations in WPA-Enterprise authentication methods and a lack of user diligence in recognizing security warnings related to untrusted certificates [14]. These issues underscore the critical need for robust user education and more intuitive, secure configuration defaults in enterprise Wi-Fi deployments [14].

VII. WPS VULNERABILITIES AND EXPLOITATION:

The Wi-Fi Protected Setup feature, designed to simplify wireless network setup, unfortunately introduced significant security vulnerabilities due to its inherent design flaws, particularly in its PIN-based authentication mechanism. This design flaw allows for efficient brute-force attacks against the PIN, significantly compromising the security of networks that utilize this feature [30].

Specifically, the WPS PIN is divided into two smaller, independently verifiable halves, allowing an attacker to determine each half separately with far fewer attempts than would be required for the full 8-digit PIN [31]. This design decision reduces the effective keyspace for a brute-force attack from 10^8 to roughly 10^4 + 10^3 combinations, making it feasible to crack the PIN in a matter of hours [15].

VIII. ADVANCES IN WPA3 SECURITY:

WPA3 was introduced to mitigate the inherent weaknesses found in its predecessors, particularly by replacing the problematic four-way handshake with the more secure Simultaneous Authentication of Equals handshake. This advancement, known as SAE, offers enhanced protection against offline dictionary attacks and improves forward secrecy, making it significantly harder for attackers to deduce network passwords even if they compromise a session key. Furthermore, WPA3 mandates the use of 192-bit cryptographic strength in its Enterprise mode, aligning with the Commercial National Security Algorithm suite to provide robust protection for sensitive data. Additionally, WPA3 introduces Enhanced Open, which offers individualized data encryption in open, unauthenticated networks, thereby preventing passive eavesdropping and providing a baseline level of privacy where none existed before.

This critical feature elevates the security posture of public Wi-Fi networks by encrypting traffic between individual clients and the access point, thereby safeguarding user privacy against pervasive surveillance techniques [32]. Consequently, transitioning to WPA3 requires careful planning and execution to ensure seamless integration and continued network availability while maximizing security benefits.

IX. COMMON WIRELESS ATTACK VECTORS (DOS, DDOS, BRUTE-FORCE):

While the advancements in WPA3 offer enhanced protection, various attack vectors continue to threaten wireless networks, necessitating a comprehensive understanding of these vulnerabilities. These vectors range from sophisticated denial-of-service and distributed denial-of-service attacks aimed at disrupting network availability to more targeted security breaches designed to exfiltrate sensitive data or gain unauthorized access. Attackers frequently leverage techniques such as KRACK attacks against WPA2 by retransmitting the third handshake message, which can lead to the reinstallation of encryption keys and subsequent decryption of network traffic [30].

Furthermore, impersonation attacks, where an adversary mimics a legitimate device to gain unauthorized access or manipulate network

communications, remain a significant concern, even with robust encryption protocols [4].
Therefore, implementing comprehensive security measures, including intrusion detection and prevention systems, becomes paramount to safeguard against these pervasive threats.

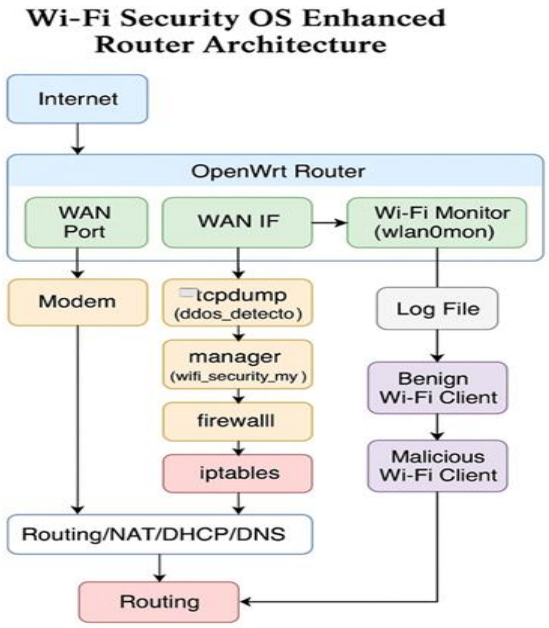
X. EXISTING INTRUSION DETECTION AND PREVENTION SYSTEMS FOR WIRELESS NETWORKS:

Current intrusion detection and prevention systems for wireless networks often rely on signature-based detection, behavioral analysis, and anomaly detection to identify and mitigate malicious activities [11] [3]. Signature-based systems, while effective against known threats, struggle with zero-day attacks, whereas behavioral and anomaly detection methods, by profiling normal network activity, can identify deviations indicative of novel threats [11].
However, these systems often face challenges related to high false positive rates, computational overhead, and the complexity of distinguishing legitimate network fluctuations from actual threats, especially in dynamic wireless environments. The integration of generative AI in intrusion detection systems offers a promising avenue to address these limitations by creating synthetic attack patterns for training, thereby enhancing the IDS's resilience against diverse and evolving threats [33].
Hence, Generative AI can optimize security in next-generation communication systems by facilitating proactive security postures through the generation of synthetic attack data, thereby expanding the range of scenarios that Intrusion Detection Systems can experience and learn from [34].

XI. RESEARCH METHODOLOGY:

The study employs a qualitative, analytical, and implementation-based methodological framework to scrutinize Wi-Fi security protocols and gauge the efficacy of router-level active defence mechanisms. The methodology is structured into three clearly defined phases. During the initial phase, the list of the wireless protocols scrutinized includes WPA, WPA2, WPS, and WPA3. This step involved the examination of authentication workflows, encryption mechanisms, and documented vulnerabilities by using standard specifications and existing sources of academic literature. The purpose of this is to recognize the security gaps that still exist even after the cryptographic advancements.
Practically evaluate the testing in an OpenWRT-based environment was the next step of the process. A router setting up OpenWRT has been used to watch the network behavior both in normal and in attack-like traffic conditions. Package monitoring tools, together with system logs, were used to investigate traffic patterns and detect abnormal activity to apply blocking by means of firewall mechanisms. This phase has been more oriented to router-level monitoring rather than to end-device safety.
The last phase was the correlation of theoretical vulnerabilities and practical behaviors. The result of monitoring, logging, and mitigation activities was analyzed for effectiveness and impact on performance as far as its applicability is concerned. This way, the findings remain focused on both theoretical and practical aspects.

XII. SYSTEM ARCHITECTURE DESIGN:



The proposed Wi-Fi Security OS Enhanced Router Architecture is built on the OpenWrt platform, a Linux-based router OS that allows high flexibility in packet filtering, monitoring, and logging. The architecture is modular, separating monitoring, detection, and mitigation functionalities, and ensures

compatibility with existing networking standards like NAT, DHCP, and DNS.

XIII. COMPONENT-LEVEL DESCRIPTION:

Internet Gateway:
The architecture begins with a typical Internet gateway that connects the OpenWrt router to the broader internet via the WAN Port. Data from the external network flows into the WAN Interface (WAN IF).
Monitoring and Detection Modules:
The Wi-Fi Monitor (wlan0mon) operates in monitor mode, passively capturing packets on the wireless interface. These packets are simultaneously logged and forwarded to tcpdump, a lightweight packet analysis tool configured with a DDoS detection script (ddos_detecto).

XIV. SECURITY MANAGEMENT AND DECISION LOGIC:

Captured packets are analyzed by a custom manager script, referred to here as wifi_security_my, responsible for classifying network behavior. This script interprets tcpdump data to differentiate between benign Wi-Fi clients and malicious actors based on predefined thresholds (e.g., packet flooding, spoofing attempts).
The Log File subsystem stores monitoring outcomes, offering a historical audit trail for forensic analysis.

XV. FIREWALL AND RULE ENFORCEMENT:

Detected threats are escalated to firewalld, a dynamic firewall daemon. It dynamically updates iptables rules, implementing immediate mitigation strategies, such as blocking IP addresses or disabling suspicious interfaces.

XVI. PACKET HANDLING AND CORE NETWORKING SERVICES:

Packets that pass security verification are routed to standard network functions such as Routing, NAT (Network Address Translation), DHCP, and DNS. This ensures seamless connectivity for verified clients while isolating or dropping malicious traffic.
The final Routing stage ensures legitimate traffic is forwarded to appropriate local or external destinations.
The proposed system architecture will integrate a TP-Link Archer T2 Plus adapter with a Wi-Fi router equipped with a USB port, facilitating real-time monitoring and active blocking of malicious traffic based on MAC addresses. This design aims to create a robust intrusion prevention system that actively monitors incoming traffic for anomalies indicative of DDoS, DoS, or other security breaches, utilizing the adapter for enhanced data capture and analysis.
This approach allows for granular control over network traffic, enabling the system to dynamically identify and block malicious MAC addresses associated with identified threats, thereby mitigating attacks at the source. However, the effectiveness of such a system heavily relies on its ability to accurately detect evolving attack patterns and differentiate them from legitimate network traffic, a task where traditional methods often fall short.

XVII. FINDINGS AND RESULTS:

The data here reveals that WPA3 is a vast improvement over brute-force attacks, offline dictionary, or both, but does not necessarily protect against any form of availability attacks such as a deauthentication flood or traffic saturation. Compared to WPA2, along with WPS, even the weakest settings or compatibility issues have shown such networks to be more susceptible. It was noticed through hands-on testing using the OpenWRT-based setup that unusual traffic patterns, or say abrupt spurt in the packet transmission figure or login attempts, could be identified without any requirement to decode the transactions. It is feasible as the router or the network could identify normal activities from any illicit action. Dynamic firewall rule augmentation made possible quick isolation of malicious devices, reducing the effects of an attack on the network while maintaining connections from the end-users. Analysis of system resource consumption indicated minor performance degradation, indicative of the efficacy of this approach on resource-constrained routers. Overall, the results reaffirm that the need for router-based remedies in order to enhance Wi-Fi network security.

XVIII. DISCUSSION:

Results from this study further accentuate the need for shifting Wi-Fi security paradigms from exclusively

protocol-centered designs to integrated, router-level defense mechanisms. While WPA3 and other advances remedy important cryptographic vulnerabilities, real-world threats are rapidly exploiting availability in addition to confidentiality. An OpenWRT-based approach, as described in this paper, illustrates active monitoring and enforcement at the access point that naturally complement other existing security standards.

This work underlines that the effectiveness of security depends not only on the robustness of the protocol but also on deployment architecture and the ability to respond to incidents. By making the router an active security entity, wireless networks can more effectively adjust to an evolving threat landscape. Further research may develop the inclusion of intelligent detection mechanisms and the extension of protections to further attack categories with the objective of even stronger wireless network security.

XIX. CONCLUSION:

In this paper, the researchers explore the landscape of security in modern Wi-Fi networks through the strengths and weaknesses of some widely deployed security protocols, namely WPA, WPA2, WPS, and WPA3. Successive updates to these protocols have significantly enhanced their encryption and authentication mechanisms. Results, however, show that protocol-level security alone cannot safeguard wireless networks against availability-based threats like deauthentication, DoS, and DDoS attacks. These threats exploit passive features of conventional Wi-Fi access points, eventually compromising network reliability and user experience.

To mitigate this deficiency, this study proposes and evaluates a router-level active defense framework built on top of the OpenWRT platform. The proposed framework will enable real-time traffic monitoring, behavioral observation, and dynamic firewall enforcement at the access point, turning the Wi-Fi router from an originally passive forwarding device into an active security agent. Empirical experiments and analysis demonstrate that abnormal traffic patterns can be identified through traffic metadata and connection behavior, enabling the isolation of malicious devices without disrupting legitimate network usage. It is observed that this is feasible within the resource constraints of consumer-grade routers.

This work argues that a multilayered model of security-one that incorporates protocol-level protections with router-resident monitoring and mitigation-is necessary for practically robust Wi-Fi security. WPA3 indeed represents a major leap in wireless security, but the fact remains that its overall effectiveness is significantly amplified when combined with network-edge-based active defenses. This work highlights how community-supported, open-source platforms such as OpenWRT may play a leading role in future wireless security designs. Future work can build upon this framework to include adaptive detection techniques and expanded attack coverage, allowing Wi-Fi networks of the future to be more resilient against the rapidly changing cyber landscape in ever-connected environments.

XX. SUMMARY OF KEY FINDINGS:

WPA3 enhances confidentiality and authentication but does not comprehensively mitigate attacks focused on availability.WPS remains a significant security risk due to fundamental flaws in its design. Router-level traffic monitoring can support the early detection of anomalous behaviors without deep packet inspection. OpenWRT is flexible enough to implement active monitoring and mitigation mechanisms. Protocol-level security combined with router-level enforcement greatly enhances overall network resilience.

REFERENCES:

[1] H. Alamleh, L. Estremera, S. S. Arnob, and A. A. S. AlQahtani, “Advanced Persistent Threats and Wireless Local Area Network Security: An In-Depth Exploration of Attack Surfaces and Mitigation Techniques,” Journal of Cybersecurity and Privacy, vol. 5, no. 2, p. 27, May 2025, doi: 10.3390/jcp5020027

[2] A. Halbouni, L.-Y. Ong, and M.-C. Leow, “Wireless Security Protocols WPA3: A Systematic Literature Review,” IEEE Access, vol. 11, p. 112438, Jan. 2023, doi: 10.1109/access.2023.3322931

[3] H. Aden et al., “WG5: Legal factors in cybersecurity for wireless systems: a vertical approach,” Research Portal Denmark, p. 67,

Jan. 2025, Accessed: Jul. 2025. [Online]. Available: https://local.forskningsportal.dk/local/dki-cgi/ws/cris-link?src=aau&id=aau-16b9f1f7-9c21-47c5-9610-b70ae3b6540c&ti=WG5%20%3A%20Legal%20factors%20in%20cybersecurity%20for%20wireless%20systems%3A%20a%20vertical%20approach

[4] L. F. Abanto-Leon, A. Baeuml, G. Hong, M. Hollick, and A. Asadi, "Stay Connected, leave no Trace," arXiv (Cornell University), vol. 4, no. 3, p. 1, Nov. 2020, Accessed: Aug. 2025. [Online]. Available: http://arxiv.org/abs/2011.12644

[5] K. Ramezanpour, J. Jagannath, and A. Jagannath, "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," Computer Networks, vol. 221, p. 109515, Dec. 2022, doi: 10.1016/j.comnet.2022.109515

[6] L. F. Abanto-Leon, A. Bäuml, G. H. Sim, M. Hollick, and A. Asadi, "Stay Connected, Leave no Trace," Proceedings of the ACM on Measurement and Analysis of Computing Systems, vol. 4, no. 3, p. 1, Nov. 2020, doi: 10.1145/3428329

[7] A. S. Abrar, N. Patwari, and S. K. Kasera, "Quantifying Interference-Assisted Signal Strength Surveillance of Sound Vibrations," IEEE Transactions on Information Forensics and Security, vol. 16, p. 2018, Dec. 2020, doi: 10.1109/tifs.2020.3045316

[8] M. Silva, J. L. Santos, and M. Curado, "The Path Towards Virtualized Wireless Communications: A Survey and Research Challenges," Journal of Network and Systems Management, vol. 32, no. 1, Nov. 2023, doi: 10.1007/s10922-023-09788-3

[9] M. K. U. Khan, "An intelligent transportation system for forecasting wireless communication network issues with cyber-attacks," Journal of Engineering Research, Nov. 2021, doi: 10.36909/jer.11881

[10] M. A. Awan, Y. Dalveren, F. Ö. Çatak, and A. Kara, "Deployment and Implementation Aspects of Radio Frequency Fingerprinting in Cybersecurity of Smart Grids," Electronics , vol. 12, no. 24, p. 4914, Dec. 2023, doi: 10.3390/electronics12244914

[11] S. N. Pujar, G. Choudhary, S. K. Shandilya, V. Sihag, and A. Choudhary, "An Adaptive Auto Incident Response based Security Framework for Wireless Network Systems," Research Portal Denmark, vol. 7, Jan. 2021, doi: 10.22667/rebicte.2021.08.15.004

[12] Y. Z. Lim, H. B. A. Rahman, and B. Sikdar, "False Sense of Security on Protected Wi-Fi Networks," arXiv (Cornell University) , Jan. 2025, doi: 10.48550/arxiv.2501.13363

[13] A. Bartoli, "Understanding Server Authentication in WPA3 Enterprise," Applied Sciences, vol. 10, no. 21, p. 7879, Nov. 2020, doi: 10.3390/app10217879

[14] I. Palamà, A. Amici, G. Bellicini, F. Gringoli, F. Pedretti, and G. Bianchi, "Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments," Computer Communications , vol. 212, p. 129, Sep. 2023, doi: 10.1016/j.comcom.2023.09.031

[15] A. Muñoz, C. Fernández-Gago, and R. López-Villa, "A Test Environment for Wireless Hacking in Domestic IoT Scenarios," Mobile Networks and Applications , vol. 28, no. 4, p. 1255, Oct. 2022, doi: 10.1007/s11036-022-02046-x

[16] E. Chatzoglou, G. Kambourakis, and C. Kolias, "How is your Wi-Fi connection today? DoS attacks on WPA3-SAE," Journal of Information Security and Applications , vol. 64, p. 103058, Dec. 2021, doi: 10.1016/j.jisa.2021.103058

[17] A. Allen, A. Mylonas, S. Vidalis, and D. Gritzalis, "Smart homes under siege: Assessing the robustness of physical security against wireless network attacks," Computers & Security , vol. 139, p. 103687, Dec. 2023, doi: 10.1016/j.cose.2023.103687

[18] Z. Luo, W. Wang, Q. Huang, T. Jiang, and Q. Zhang, "Securing IoT Devices by Exploiting Backscatter Propagation Signatures," IEEE Transactions on Mobile Computing, vol. 21, no. 12, p. 4595, Jun. 2021, doi: 10.1109/tmc.2021.3084754

[19] Q.-T. Dao, N. T. T. Loan, T.-I. Ha, V.-H. Nguyen, and T. A. Nguyen, "Investigation of Secure Communication of Modbus TCP/IP Protocol: Siemens S7 PLC Series Case Study," Applied System Innovation, vol. 8, no. 3, p. 65, May 2025, doi: 10.3390/asi8030065

[20] F. Martínez et al., "Redefining DDoS Attack Detection Using A Dual-Space Prototypical Network-Based Approach," arXiv (Cornell University) , Jun. 2024, doi: 10.48550/arxiv.2406.02632

[21] L. Bi, Z. Xu, and L. Yang, "Low-cost UAV detection via WiFi traffic analysis and machine learning," Scientific Reports , vol. 13, no. 1, Nov. 2023, doi: 10.1038/s41598-023-47453-6

[22] G. Granato, A. Martino, A. Baiocchi, and A. Rizzi, "Graph-Based Multi-Label Classification for WiFi Network Traffic Analysis," Applied Sciences, vol. 12, no. 21, p. 11303, Nov. 2022, doi: 10.3390/app122111303

[23] M. A. Uddin, S. Aryal, M. R. Bouadjenek, M. Al-Hawawreh, and Md. A. Talukder, "usfAD based effective unknown attack detection focused IDS framework," Scientific Reports , vol. 14, no. 1, Nov. 2024, doi: 10.1038/s41598-024-80021-0

[24] X. Fang et al. , "Pioneering advanced security solutions for reinforcement learning-based adaptive key rotation in Zigbee networks," Scientific Reports , vol. 14, no. 1, Jun. 2024, doi: 10.1038/s41598-024-64895-8

[25] [25] R. Kalaria, A. S. M. Kayes, W. Rahayu, E. Pardede, and A. S. S., "IoTPredictor: A security framework for predicting IoT device behaviours and detecting malicious devices against cyber attacks," Computers & Security , vol. 146, p. 104037, Aug. 2024, doi: 10.1016/j.cose.2024.104037

[26] B. Tushir, V. K. Ramanna, Y. Liu, and B. Dezfouli, "Leveraging Machine Learning for Accurate IoT Device Identification in Dynamic Wireless Contexts," arXiv (Cornell University) , May 2024, doi: 10.48550/arxiv.2405.17442

[27] A. Mishra, A. C. Viana, and N. Achir, "Bleach: From WiFi probe-request signatures to MAC association," Ad Hoc Networks, vol. 164, p. 103623, Aug. 2024, doi: 10.1016/j.adhoc.2024.103623

[28] W. S. Admass, Y. Y. Munaye, and A. Diro, "Cyber security: State of the art, challenges and future directions," Cyber Security and Applications, vol. 2, p. 100031, Oct. 2023, doi: 10.1016/j.csa.2023.100031

[29] P. Park, P. D. Marco, J. Nah, and C. Fischione, "Wireless Avionics Intracommunications: A Survey of Benefits, Challenges, and Solutions," IEEE Internet of Things Journal, vol. 8, no. 10, p. 7745, Nov. 2020, doi: 10.1109/jiot.2020.3038848

[30] O. Stan et al., "Extending Attack Graphs to Represent Cyber-Attacks in Communication Protocols and Modern IT Networks," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, p. 1936, Dec. 2020, doi: 10.1109/tdsc.2020.3041999

[31] V. Kampourakis, E. Chatzoglou, G. Kambourakis, A. Dolmes, and C. Zaroliagis, "WPAxFuzz: Sniffing Out Vulnerabilities in Wi-Fi Implementations," Cryptography, vol. 6, no. 4, p. 53, Oct. 2022, doi: 10.3390/cryptography6040053

[32] E. C. Rye and D. Levin, "Surveilling the Masses with Wi-Fi-Based Positioning Systems," arXiv (Cornell University) , May 2024, doi: 10.48550/arxiv.2405.14975

[33] T.-H. Vu, S. K. Jagatheesaperumal, M.-D. Nguyen, N. V. Huynh, S. Kim, and Q. Pham, "Applications of Generative AI (GAI) for Mobile and Wireless Networking: A Survey," arXiv (Cornell University), May 2024, doi: 10.48550/arxiv.2405.20024

[34] F. Khoramnejad and E. Hossain, "Generative AI for the Optimization of Next-Generation Wireless Networks: Basics, State-of-the-Art, and Open Challenges," arXiv (Cornell University), May 2024, doi: 10.48550/arxiv.2405.17454

[35] F. L. de C. Filho et al., "Botnet Detection and Mitigation Model for IoT Networks Using Federated Learning," Sensors, vol. 23, no. 14, p. 6305, Jul. 2023, doi: 10.3390/s23146305

[36] M. Zang, C. Zheng, L. Dittmann, and N. Zilberman, "Toward Continuous Threat Defense: in-Network Traffic Analysis for IoT Gateways," IEEE Internet of Things Journal, vol. 11, no. 6, p. 9244, Oct. 2023, doi: 10.1109/jiot.2023.3323771

[37] M. H. Moharam, K. Ashraf, H. Alaa, M. Ahmed, and H. A. El-Hakim, "Real-time detection of Wi-Fi attacks using hybrid deep learning models on NodeMCU," Scientific Reports, vol. 15, no. 1, Sep. 2025, doi: 10.1038/s41598-025-18947-2

[38] M. A. Akhtar, S. M. O. Qadri, M. A. Siddiqui, S. M. N. Mustafa, S. Javaid, and S. A. Ali, "Robust genetic machine learning ensemble model for intrusion detection in network traffic," Scientific Reports, vol. 13, no. 1, Oct. 2023, doi: 10.1038/s41598-023-43816-1

[39] K. Alanezi and S. Mishra, "An IoT Architecture Leveraging Digital Twins: Compromised Node Detection Scenario," IEEE Systems Journal, vol. 18, no. 2, p. 1224, Jun. 2024, doi: 10.1109/jsyst.2024.3403500

[40] K. Saranya and A. Valarmathi, "A multilayer deep autoencoder approach for cross layer IoT attack detection using deep learning algorithms," Scientific Reports, vol. 15, no. 1, Mar. 2025, doi: 10.1038/s41598-025-93473-9

[41] X.-H. Nguyen, X.-D. Nguyen, H.-H. Huynh, and K.-H. Le, "Realguard: A Lightweight Network Intrusion Detection System for IoT Gateways," Sensors, vol. 22, no. 2, p. 432, Jan. 2022, doi: 10.3390/s22020432

[42] H. F. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallègue, "Using machine learning algorithms to enhance IoT system security," Scientific Reports, vol. 14, no. 1, May 2024, doi: 10.1038/s41598-024-62861-y

[43] S. B. Atitallah, M. Driss, W. Boulila, and A. Koubâa, "Strengthening Network Intrusion Detection in IoT Environments with Self-Supervised Learning and Few Shot Learning," arXiv (Cornell University), Jun. 2024, doi: 10.48550/arxiv.2406.02636

[44] Z. Alwaisi, T. Kumar, E. Harjula, and S. Soderi, "Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention," Internet of Things, p. 101398, Oct. 2024, doi: 10.1016/j.iot.2024.101398.