Security and Privacy in Wi-Fi Networks: From Legacy Protocols to Next-Gen Defenses*

Aditya jha,[1], Hariharasitaraman. S[1], Radheshyam Singh[2], Gaurav Choudhary[3,†], and Nicola Dragoni[3]

[1] VIT Bhopal University, Madhya Pradesh, India
{aditya955559,hariharasitaraman}@gmail.com
[2] FORCE Technology, Hørsholm, Denmark
rds@forcetechnology.com
[3] Technical University of Denmark, Lyngby, Denmark
gauch@dtu.dk, ndra@dtu.dk

Abstract

Wi-Fi has become the backbone of wireless connectivity across homes, enterprises, and industrial systems, but its ubiquity makes it a constant target for security threats. This paper reviews the evolution of Wi-Fi security protocols from WEP and WPA to WPA2 and WPA3, highlighting vulnerabilities like KRACK, FragAttacks, Dragonblood, and Evil Twin attacks. It further explores privacy issues including MAC address tracking, device fingerprinting, and flaws in randomization mechanisms. Special attention is given to Industrial IoT (IIoT) environments, where resource-constrained devices and legacy protocols heighten risk. We evaluate defense strategies including WPA3 features, intrusion detection systems (WIDS), machine learning-based anomaly detection, and formal verification. Through synthesis of real-world exploits, protocol analysis, and academic work, the paper identifies persistent challenges and research gaps, while outlining future directions for building secure, resilient, and privacy-preserving Wi-Fi systems aligned with next-generation standards.

keywords: Wi-Fi Security, WPA3, KRACK, FragAttacks, Intrusion Detection, MAC Randomization, IIoT, Wireless Privacy, WPA2, Machine Learning, IEEE 802.11, WEP, WPA, Formal Verification, Evil Twin Attack, Wireless Encryption, Device Fingerprinting, IDS, Protocol Vulnerability, Network Defense

1 Introduction

Wi-Fi, based on the IEEE 802.11 standard, has become the primary wireless access medium, supporting over 20 billion devices as of 2024. With ongoing advancements like Wi-Fi 6 (802.11ax) and the upcoming Wi-Fi 7 (802.11be), its role in smart homes, industry, healthcare, and public services continues to expand [20]. However, this ubiquity makes Wi-Fi a persistent target for attackers. Its open transmission medium and legacy protocol support introduce multiple vulnerabilities, even as security standards have evolved from WEP to WPA2 and WPA3 [7, 5].

Practical attacks such as KRACK, FragAttacks, and Kr00k have exposed weaknesses in protocol design and implementation, impacting millions of devices globally and prompting

*Proceedings of The 2025 IFIP WG 8.4 International Symposium on E-Business Information Systems Evolution (EBISION 2025), Article No. 25, December 16-18, 2025, Sapporo, Japan. © The copyright of this paper remains with the author(s).

†Corresponding author

standardization bodies like IEEE and the Wi-Fi Alliance to revise their security postures [1, 3, 4, 5, 7]. Beyond these, advanced threats like Evil Twin attacks, rogue APs, and side-channel exploits pose serious risks, especially in open or semi-secure environments like airports and public hotspots [16].

Privacy concerns have also intensified. Despite MAC address randomization and Protected Management Frames (PMF), devices remain traceable through timing signatures, static elements in probe frames, and side-channel metadata [6, 15]. This allows adversaries to fingerprint and track users, even when privacy features are enabled.

The rise of Industrial IoT (IIoT) adds another dimension to Wi-Fi security. Low-power devices often lack robust encryption or timely updates, making them vulnerable to persistent threats. Weak authentication and poor configurations in industrial environments can lead to data breaches and system disruptions [13, 14].

In light of these concerns, this paper presents a comprehensive review of the Wi-Fi security landscape, focusing on:

- Evolution of Wi-Fi protocols and their comparative strengths,
- Documented vulnerabilities and real-world attacks,
- Modern privacy threats and device tracking methods,
- Security challenges in IoT and IIoT environments,
- Emerging defenses including protocol enhancements, intrusion detection, formal verification, and ML-based solutions [9, 11, 12].

Drawing on current research, specifications, and practical findings, this review offers a holistic, forward-looking perspective to help guide future wireless security development.

2 Evolution of Wi-Fi Security Protocols

The security of Wi-Fi networks has evolved significantly since the inception of the IEEE 802.11 standard in 1997. Each generation of security protocols—WEP, WPA, WPA2, and WPA3—has aimed to address vulnerabilities discovered in previous iterations, while balancing performance, usability, and backward compatibility [7]. This section outlines the historical progression and core technical features of each protocol, highlighting their respective strengths and weaknesses.

As shown in Fig. 1, the evolution from WEP to WPA3 highlights a progressive enhancement in cryptographic design, protocol robustness, and resistance to modern attack vectors [5].

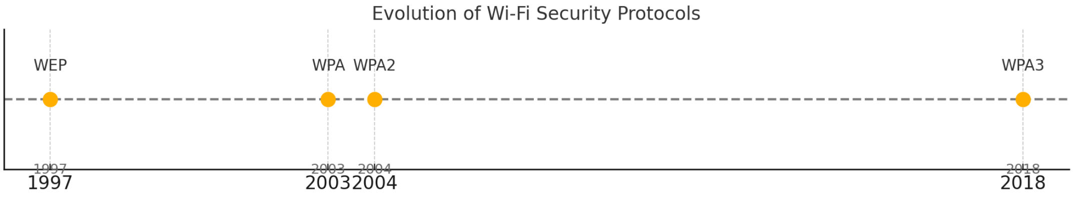

Figure 1: Timeline of Wi-Fi security protocol evolution from WEP (1997) to WPA3 (2018).

Wired Equivalent Privacy (WEP): WEP was the original security protocol introduced with IEEE 802.11 to provide confidentiality comparable to wired networks. It utilized the RC4 stream cipher for encryption and a 24-bit Initialization Vector (IV) combined with a shared secret key [7]. Despite its widespread early adoption, WEP suffered from critical flaws. The limited IV space resulted in frequent key reuse, and statistical attacks could recover the key with minimal packet capture. The Fluhrer–Mantin–Shamir (FMS) attack and its variants demonstrated that WEP keys could be cracked within minutes using tools such as Aircrack-ng. Due to these vulnerabilities, the IEEE deprecated WEP in 2004.

Wi-Fi Protected Access (WPA): To address WEP's shortcomings, the Wi-Fi Alliance introduced WPA in 2003 as an interim solution [5]. WPA retained the RC4 cipher but introduced the Temporal Key Integrity Protocol (TKIP), which included per-packet key mixing, a message integrity check (MIC), and a replay protection mechanism [8]. While WPA improved security, it was still based on legacy cryptography. Subsequent attacks, such as the Beck–Tews and Ohigashi–Morii attacks, exploited weaknesses in TKIP's design, enabling packet injection and decryption under specific conditions. Consequently, TKIP has been officially deprecated by IEEE and should not be used in modern deployments.

Wi-Fi Protected Access II (WPA2)

WPA2, standardized as IEEE 802.11i in 2004, marked a major advancement in wireless security [7]. It replaced RC4/TKIP with the Advanced Encryption Standard (AES) using the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). WPA2 supports both personal (Pre-Shared Key) and enterprise (802.1X) modes, offering scalable security for a wide range of use cases. WPA2 was considered secure for over a decade, but multiple implementation-level vulnerabilities were later discovered. The most notable was the Key Reinstallation Attack (KRACK), which exploited weaknesses in the four-way handshake to reinstall encryption keys, allowing an adversary to decrypt traffic [1]. Despite the robustness of AES-CCMP, WPA2's reliance on correct implementation and configuration exposed it to real-world attacks.

Wi-Fi Protected Access III (WPA3):Introduced in 2018, WPA3 addresses WPA2's shortcomings with stronger security features [5]. It replaces PSK with Simultaneous Authentication of Equals (SAE), offering forward secrecy and resistance to offline dictionary attacks [2]. WPA3 mandates Protected Management Frames (PMF) to prevent deauthentication attacks, supports Opportunistic Wireless Encryption (OWE) for open networks [18], and offers a 192-bit security suite for high-assurance environments. Despite these advances, early WPA3 implementations were vulnerable to side-channel attacks like Dragonblood, which exploited weaknesses in SAE for password recovery or downgrade [2]. While patches have mitigated these risks, ongoing refinement by the Wi-Fi Alliance remains essential [5].

Table 1: Compact Summary of Wi-Fi Security Protocol Features

Protocol	**Cipher**	**Handshake**	**Key Takeaways**
WEP	RC4	None	Deprecated due to weak IV reuse, vulnerable to FMS attacks
WPA	RC4 (TKIP)	4-Way TKIP	Interim fix with per-packet keys, but legacy cipher vulnerabilities persist
WPA2	AES-CCMP	4-Way AES	Long-standing standard with strong encryption, but susceptible to KRACK if misconfigured
WPA3	AES-GCMP, 192-bit	SAE (Dragonfly)	Strong resistance to offline attacks, mandatory PMF, and support for forward secrecy

Table 1 presents a high-level comparison of the four major Wi-Fi security protocols.

In addition to the tabular overview, a visual comparison of security features is illustrated in Fig. 2, offering an intuitive understanding of the relative strengths of each protocol.

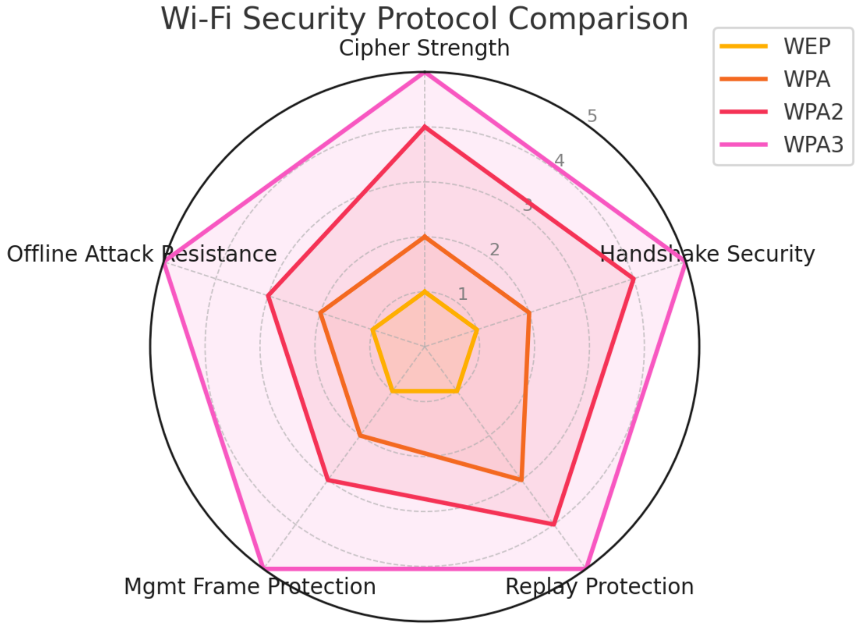

Figure 2: Radar chart comparing Wi-Fi security protocols across key features including cipher strength, handshake security, replay protection, management frame protection, and offline attack resistance.

The evolution of Wi-Fi security protocols reflects the dynamic threat landscape and the continuous efforts of standardization bodies to adapt. While WPA3 addresses many legacy vulnerabilities, secure implementation, timely updates, and adherence to best practices remain critical to maintaining wireless network integrity [3, 4].

3 Vulnerabilities and Real-World Attacks

Despite ongoing advancements in Wi-Fi security protocols, practical attacks have continued to surface due to both protocol design flaws and insecure implementations. This section reviews the major vulnerabilities that have affected Wi-Fi networks, highlighting how attackers have exploited cryptographic weaknesses, implementation oversights, and client behavior to compromise data confidentiality, integrity, and availability [1, 2, 3, 4].

As shown in Fig. 3, Wi-Fi vulnerabilities can be categorized based on their origin in the protocol stack—ranging from design-level flaws to physical-layer threats [16, 15].

Key Reinstallation Attack (KRACK):Discovered by Vanhoef and Piessens in 2017, the Key Reinstallation Attack (KRACK) exploits a vulnerability in the WPA2 four-way handshake [1]. During key exchange, an attacker can replay message 3 to force the victim to reinstall an already-in-use key, resetting associated nonce and replay counters. This nonce reuse violates the assumptions of AES-CCMP, allowing attackers to decrypt or manipulate packets.

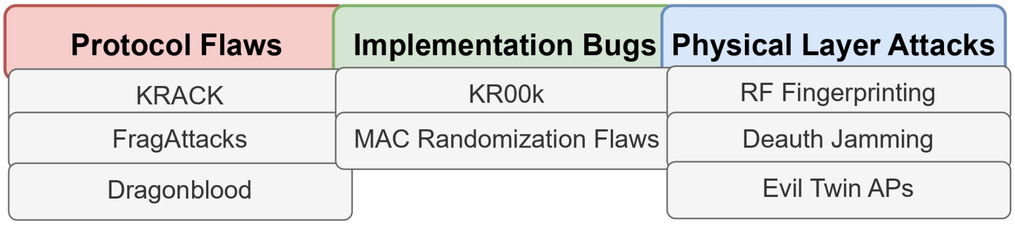

Figure 3: Layered classification of major Wi-Fi security vulnerabilities across protocol design flaws, implementation bugs, and physical-layer attacks.

KRACK affected virtually all WPA2-compliant devices and highlighted the criticality of implementation correctness even when protocols are cryptographically sound. It was mitigated via firmware updates that enforce nonce reuse checks and restrict key reinstallations.

Fragmentation and Aggregation Attacks (FragAttacks): In 2021, Vanhoef disclosed a new class of attacks called FragAttacks, targeting frame fragmentation and aggregation features in IEEE 802.11 [3]. These attacks exploit how receivers handle mixed encrypted and plaintext fragments or aggregate frames with overlapping data.

FragAttacks can enable:

- Injection of plaintext frames into encrypted streams,
- Bypassing of firewall rules via crafted frame structures,
- Remote code execution on vulnerable devices.

The vulnerabilities stemmed from protocol ambiguities and were present in both WPA2 and WPA3 implementations. Mitigation required both firmware updates and improved device-side input validation.

KR00k KR00k is a vulnerability disclosed in 2020 that affected Wi-Fi chips from Broadcom and Cypress [4]. When a device disconnected from an access point, some chipsets would erroneously transmit remaining buffered data encrypted with an all-zero key.

This allowed attackers to force disassociation (e.g., using deauthentication frames) and capture sensitive data sent post-disconnection. KR00k was resolved through firmware patches but highlighted the risks posed by low-level chipset behavior.

Dragonblood Attacks on WPA3 Though WPA3 was designed to address WPA2's limitations, early implementations of its Simultaneous Authentication of Equals (SAE) handshake were found to be susceptible to side-channel and downgrade attacks.

Dragonblood, a set of attacks published in 2019, demonstrated [2]:

- Timing side-channels in SAE's password element derivation,
- Downgrade attacks that forced WPA3-capable devices into WPA2 mode,
- Resource exhaustion via invalid curve attacks.

Vendors responded with patched firmware and improved SAE implementations. Dragonblood emphasized the need for side-channel resistance and robust transition mode handling in WPA3.

Rogue Access Points and Evil Twin Attacks: Rogue access point (AP) attacks, especially Evil Twin scenarios, involve adversaries setting up fake APs that mimic legitimate networks [16]. Unsuspecting clients may auto-connect or be tricked into joining the rogue AP, enabling man-in-the-middle (MitM) attacks.

Attackers can:

- Intercept and manipulate traffic,
- Phish for credentials using fake captive portals,
- Force device associations using deauthentication and signal jamming.

These attacks are particularly effective in open or poorly secured public networks. Even WPA2-protected clients are vulnerable if the SSID is shared and no server certificate verification is enforced.

Side-Channel and Implementation Attacks: Several additional classes of vulnerabilities exploit side-channels or implementation-specific weaknesses:

- Timing attacks: Exploiting time variations in key handling (e.g., Dragonblood) [2].
- All-zero key bugs: As seen in KR00k and similar chipset flaws [4].
- Incorrect randomization: Leading to MAC address leaks and device fingerprinting [6, 15].

Such vulnerabilities underline the importance of robust, side-channel-hardened implementations and regular audits.

Denial-of-Service (DoS) Attacks:Wi-Fi networks remain susceptible to a variety of DoS attacks, including:

- Deauthentication flooding: Exploiting unprotected management frames (in pre-WPA3 networks),
- Beacon spamming and channel jamming Overloading the wireless medium with interference or fake networks [16].

WPA3's enforcement of Protected Management Frames (PMF) mitigates some of these issues [5, 18], but jamming and physical-layer DoS remain difficult to counter in practice.

Table 2 summarizes the major vulnerabilities and their respective targets and mitigations.

These vulnerabilities demonstrate that Wi-Fi security must be approached holistically. Protocol design, implementation rigor, and proactive monitoring are all essential to defending against evolving attack techniques.

4 Privacy Threats and MAC Address Tracking

While Wi-Fi security protocols primarily aim to protect data confidentiality and integrity, privacy remains an under-addressed yet critical concern. Modern Wi-Fi-enabled devices frequently emit signals—including probe requests, authentication frames, and association attempts—that may unintentionally leak identifying information. These emissions can be exploited by adversaries to track, fingerprint, or re-identify users across locations and time [6, 15].

Table 2: Compact Summary of Major Wi-Fi Vulnerabilities

Vulnerability	Target Protocol	Key Impact and Mitigation
KRACK	WPA2	Allows decryption and packet injection via key reuse; mitigated by firmware updates enforcing nonce validation
FragAttacks	WPA2/WPA3	Exploits frame aggregation/fragmentation for injection or remote code execution; patched via frame validation
KR00k	WPA2	Leaks encrypted frames using an all-zero key post-disassociation; resolved via chipset firmware patch
Dragonblood	WPA3	Side-channel and downgrade attacks on SAE; mitigated by implementation hardening and transition mode fixes
Evil Twin APs	All	Enables MitM, phishing via rogue AP impersonation; prevented through PMF, WIDS, and user awareness
Deauth/DoS Attacks	WEP/WPA/WPA2	Causes service disruption through jamming and spoofed management frames; mitigated using PMF and RF monitoring

4.1 MAC Address Leakage and Tracking

Wi-Fi devices use a unique 48-bit MAC address at the data link layer, which has historically been broadcast in probe and association requests, allowing easy tracking across networks and locations [15]. Passive attackers can use inexpensive tools like a Raspberry Pi to capture these broadcasts and compile movement histories without user consent. This method has been applied in public spaces such as airports and malls for surveillance and targeted marketing [6].

4.2 MAC Address Randomization and Its Limitations

MAC address randomization, adopted by platforms like Android, iOS, and Windows, replaces a device's real MAC with a temporary pseudonym during network scans to improve privacy [6]. However, its effectiveness is limited—many devices fail to randomize consistently across all scan types, and persistent randomized MACs reduce anonymity. Additionally, constant frame fields (e.g., supported rates, IEs) enable fingerprinting, while authentication may reveal the original MAC. Research confirms that devices can still be tracked using temporal patterns and signal-level characteristics despite randomization efforts [6, 15].

As illustrated in Fig. 4, even with MAC address randomization, adversaries can capture broadcasted frames and perform fingerprinting to track users across locations and time.

4.3 Device Fingerprinting via Frame Characteristics

Even with MAC randomization, devices can be fingerprinted through unique combinations of probe request features such as supported channels, information element (IE) order, vendor fields, and timing behaviors [10]. These patterns often reveal device models or OS versions and

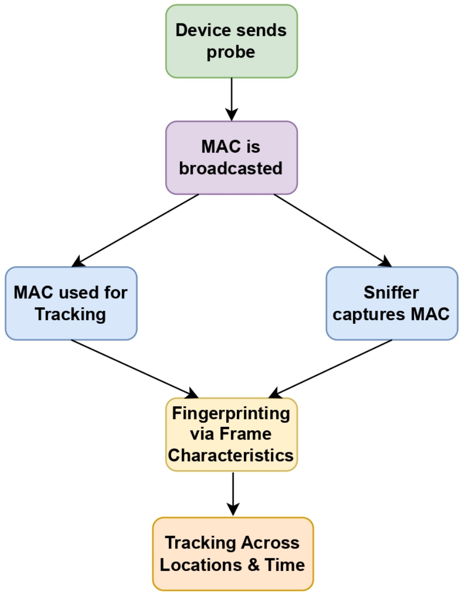

Figure 4: Flow of MAC address-based tracking. Devices broadcast MACs in probe requests, enabling sniffers to capture them and use frame characteristics for user fingerprinting and tracking.

can link multiple randomized MACs to the same user. Moreover, flaws in randomization—like fixed global addresses or shared identifiers—further weaken privacy protections [6].

4.4 Physical Layer Tracking and RF Fingerprinting

Advanced adversaries can exploit hardware-level imperfections such as Carrier Frequency Offset (CFO), phase noise, and transient signal behaviors to fingerprint a device based on its unique radio signature [15]. These radio frequency (RF) fingerprints can remain consistent across MAC changes and are especially concerning in high-surveillance environments.

Although RF fingerprinting requires more sophisticated equipment and signal processing, it demonstrates that anonymization at the software layer may not suffice to ensure wireless privacy.

4.5 Hotspot 2.0 and Privacy Trade-offs

Hotspot 2.0 (also known as Passpoint), designed to enable seamless Wi-Fi roaming, introduces new privacy risks. Devices pre-configured to auto-connect to known networks may disclose identifying information during the discovery and negotiation process. An attacker advertising a rogue Hotspot 2.0-compatible SSID could trick devices into revealing credentials or service set identifiers (SSIDs) associated with enterprise networks [19].

Without strict mutual authentication and certificate validation, these automated processes may expose users to tracking and impersonation attacks.

4.6 Real-World Implications

Wi-Fi tracking poses serious risks, enabling passive surveillance, behavioral profiling, and user de-anonymization—often without consent. It can be exploited for location analytics, security breaches in sensitive areas, or even stalking through repeated MAC address detection. These threats are especially pronounced in environments where devices constantly emit Wi-Fi signals due to background services or installed apps [15].

4.7 Mitigation Strategies

Effective Wi-Fi privacy protection demands a multi-layered approach, including short-lived randomized MACs, frame obfuscation through randomized non-essential elements, and user control over probe emissions. Regulatory policies must also enforce ethical tracking standards and consent practices [6, 19]. While ongoing research aims to balance connectivity with privacy, evolving tracking techniques continue to challenge the resilience of current mitigation strategies.

5 Wi-Fi in Industrial and IoT Environments

Wi-Fi plays a critical role in Industrial IoT (IIoT) by enabling wireless connectivity across factories, utilities, and smart infrastructure for monitoring and automation [13]. However, its integration introduces security challenges that traditional frameworks often fail to address, especially in resource-constrained environments [14]. As illustrated in Fig. 5, IIoT Wi-Fi topologies support cloud-to-device communication but are vulnerable to threats like rogue access points and unauthorized traffic injection [16].

5.1 Adoption of Wi-Fi in IIoT

Wi-Fi's broad availability, affordability, and IP compatibility make it a practical option for IIoT applications [13]. It enables mobility, flexible infrastructure, and supports use cases such as real-time monitoring in smart factories, remote diagnostics, smart meter connectivity, and wireless data offloading in logistics. However, its adoption in industrial settings also introduces new attack vectors and operational challenges due to the constrained nature of embedded devices.

5.2 Security Challenges in IIoT Deployments

IIoT devices typically operate with limited processing power, memory, and battery life, restricting their ability to perform strong encryption, manage certificates, or support timely firmware updates. These constraints also hinder real-time intrusion detection. As a result, many IIoT nodes still use outdated protocols like WPA2-PSK or insecure defaults such as open networks and hardcoded credentials, making them vulnerable to attacks like KRACK, Evil Twin, and FragAttacks [1, 3, 16].

5.3 Case Studies of IIoT Vulnerabilities

Studies have exposed several real-world flaws in industrial Wi-Fi networks [14], including unprotected access points still using outdated encryption, weak key management with shared

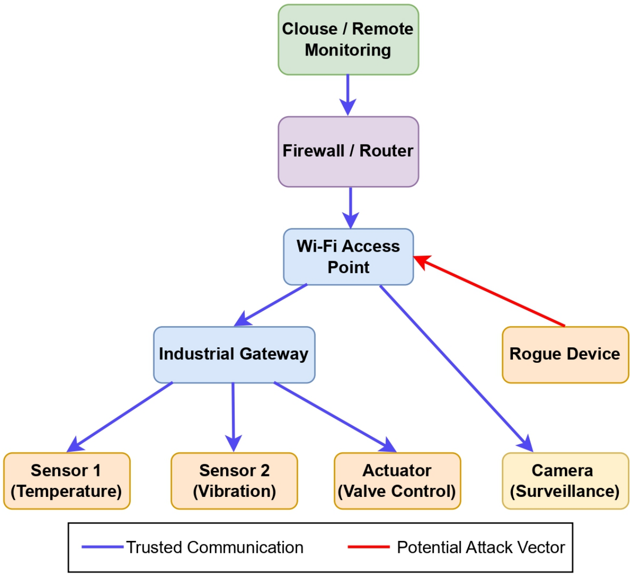

Figure 5: Typical IIoT Wi-Fi network topology showing secure communications among industrial components and a potential attack path from a rogue device.

or guessable credentials, and poor network segmentation that allows IIoT devices to coexist with enterprise systems. Additionally, misconfigured networks enable rogue device insertion, increasing the risk of unauthorized access and lateral movement [16]. Once inside, attackers can disrupt operations, alter sensor outputs, exfiltrate data, or escalate privileges within the infrastructure.

5.4 Best Practices for Securing Industrial Wi-Fi

Securing IIoT deployments requires a security-by-design approach that balances protection with device limitations. Key strategies include using WPA3-Enterprise with 802.1X authentication to block rogue APs [5], isolating IIoT devices on separate VLANs or SSIDs, and automating key rotation via protocols like DPP. Wireless IDS tools can help detect rogue devices and jamming attempts [17], while RF controls like directional antennas reduce signal leakage. These methods should be adapted for low-power and legacy devices using hybrid models that blend strong perimeter controls with lightweight protections.

5.5 Future Outlook and Standardization

As Wi-Fi 6E and Wi-Fi 7 improve latency, efficiency, and scalability for dense IIoT deployments, security must advance accordingly. Adopting standards like IEC 62443 and NIST guidelines is essential to establish strong baseline protections [19]. Growing interest in zero trust models—where every device requires continuous, contextual authentication—further emphasizes the need for dynamic, policy-driven Wi-Fi security [19]. Achieving this requires collaboration among manufacturers, architects, protocol designers, and cybersecurity teams to ensure future IIoT infrastructures remain resilient and trustworthy.

6 Countermeasures and Intrusion Detection Systems

The continuous discovery of vulnerabilities in Wi-Fi protocols and implementations highlights the need for a layered security approach that goes beyond encryption. This section surveys prominent countermeasures designed to detect, prevent, or mitigate wireless attacks, spanning from protocol-level enhancements to advanced anomaly detection systems [5, 17].

6.1 Protocol-Level Enhancements

Several enhancements have been introduced to strengthen Wi-Fi security against known attacks. WPA3 includes Simultaneous Authentication of Equals (SAE) to resist offline dictionary attacks and Opportunistic Wireless Encryption (OWE) for encrypting open traffic, while Protected Management Frames (PMF) are now mandatory to prevent deauthentication-based disruptions [5, 2, 18]. Post-KRACK and FragAttacks, vendors implemented nonce reuse checks, improved reassembly handling, and stricter packet parsing [3, 1]. Additionally, measures were taken to harden WPA3 transition mode, ensuring devices are not easily downgraded to WPA2 [2]. These improvements enhance baseline security but rely on timely and consistent adoption across diverse devices and platforms.

6.2 Wireless Intrusion Detection Systems (WIDS)

WIDS plays a vital role in wireless security by monitoring radio traffic to detect rogue APs, Evil Twin impersonations, deauthentication floods, and MAC spoofing. Tools like Kismet, AirDefense, and Cisco WIPS use distributed sensors for real-time anomaly detection, particularly in enterprise and industrial environments with centralized control [17, 16]. However, WIDS can suffer from high false positives, limited stealth detection, and challenges in analyzing encrypted traffic. Its effectiveness increases when combined with broader monitoring systems and threat intelligence platforms, enabling more contextual and reliable wireless intrusion defense.

6.3 Machine Learning-Based Detection

Machine learning (ML) is increasingly adopted to overcome the rigidity of rule-based intrusion detection systems [9, 17]. ML models can detect wireless anomalies by learning from traffic patterns and identifying irregularities in packet timing, MAC behavior, and malformed frames. Thang et al. demonstrated a multi-stage model using unsupervised clustering and outlier detection to accurately identify attacks like slow deauthentication floods and MAC spoofing [?]. Despite promising results, ML-based WIDS face challenges such as the need for high-quality training data, regular model updates, and computational optimization for low-power environments. Explainability and trust in ML decisions also remain active research areas in cybersecurity applications.

6.4 Formal Verification of Protocols

Formal methods provide a rigorous approach to verifying the correctness and security of Wi-Fi protocols. Tools like Tamarin Prover and ProVerif have modeled the WPA2 4-way handshake, WPA3-SAE, and fragmentation logic to uncover vulnerabilities such as nonce reuse and offline dictionary attack potential [11, 12, 2, 21]. These analyses have led to important protocol patches and highlighted flaws that typical testing may miss. Though computationally intensive, formal verification is invaluable for identifying logic errors, state inconsistencies, and subtle security flaws, making it a best practice in secure protocol development [21].

6.5 Best Practices for Holistic Defense

Effective Wi-Fi security demands a layered approach combining preventive controls like WPA3, strong passwords, and secure onboarding [5]; detective measures such as WIDS/WIPS and centralized logging [17]; and reactive responses like automated rogue AP isolation. Analytical tools using machine learning help predict evolving threats [9], while formal verification ensures protocol integrity [11, 12]. No single control suffices—true resilience depends on redundancy, continuous monitoring, and proactive defense.

As illustrated in Fig. 6, a layered security architecture integrates various defenses across the Wi-Fi protocol stack, from physical isolation to formal protocol verification, providing holistic protection against evolving threats.

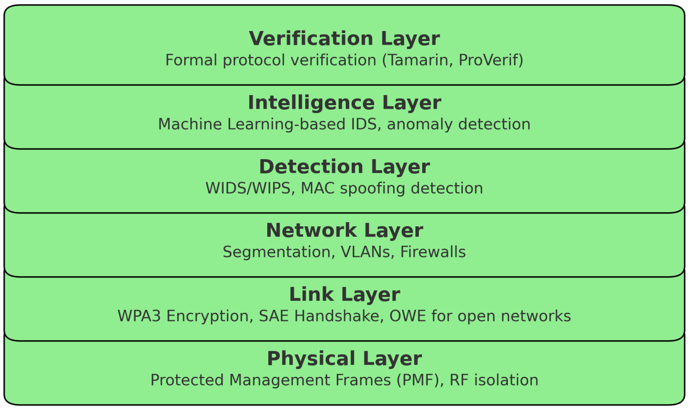
Verification Layer
Formal protocol verification (Tamarin, ProVerif)
Intelligence Layer
Machine Learning-based IDS, anomaly detection
Detection Layer
WIDS/WIPS, MAC spoofing detection
Network Layer
Segmentation, VLANs, Firewalls
Link Layer
WPA3 Encryption, SAE Handshake, OWE for open networks
Physical Layer
Protected Management Frames (PMF), RF isolation

Figure 6: Layered architecture for Wi-Fi security integrating physical-layer protections, cryptographic safeguards, intrusion detection, machine learning intelligence, and formal verification.

7 Research Gaps and Future Directions

Despite progress in protocol design, intrusion detection, and privacy mechanisms, Wi-Fi security still faces numerous unresolved challenges. With new use cases, adversarial methods, and evolving IEEE standards, continuous research is essential.

As shown in Fig. 7, future progress depends on advancing protocol resilience, ML integration, zero trust adoption, and device-level authentication.

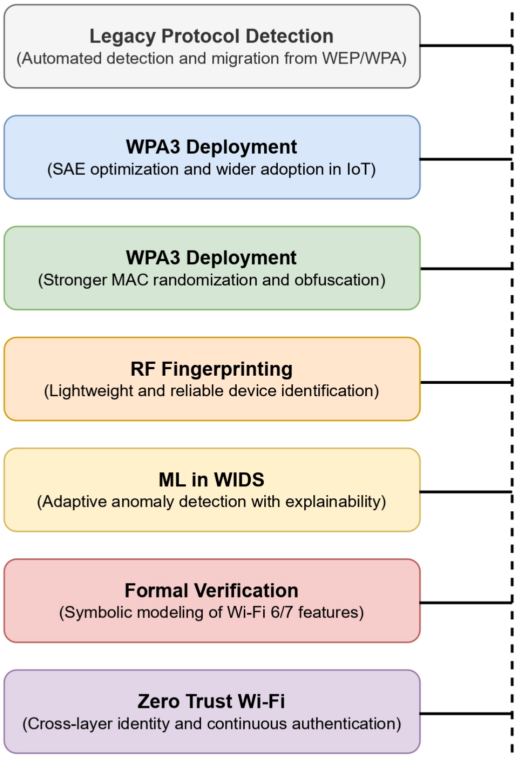
Legacy Protocol Detection
(Automated detection and migration from WEP/WPA)
WPA3 Deployment
(SAE optimization and wider adoption in IoT)
WPA3 Deployment
(Stronger MAC randomization and obfuscation)
RF Fingerprinting
(Lightweight and reliable device identification)
ML in WIDS
(Adaptive anomaly detection with explainability)
Formal Verification
(Symbolic modeling of Wi-Fi 6/7 features)
Zero Trust Wi-Fi
(Cross-layer identity and continuous authentication)

Figure 7: Future research roadmap for Wi-Fi security highlighting open challenges and priority areas such as WPA3 optimization, MAC obfuscation, ML in WIDS, formal verification, and Zero Trust frameworks.

7.1 Legacy Protocols and Insecure Deployments

Despite the availability of WPA3, many networks still operate with outdated protocols like WEP or poorly configured WPA2, exposing them to preventable attacks. These issues often stem from compatibility needs, limited awareness, or upgrade challenges in large or resource-constrained systems. Research should develop automated tools to detect insecure configurations, enforce security baselines, and enable scalable migration strategies for enterprise and IIoT environments.

7.2 Limited Adoption and Weaknesses in WPA3

Although WPA3 offers significant security improvements over its predecessors, its adoption remains limited due to device compatibility challenges, vulnerabilities in transition modes, and early weaknesses in the Simultaneous Authentication of Equals (SAE) handshake. Research should focus on strengthening downgrade resistance, optimizing SAE for low-power and legacy-constrained devices, and developing intuitive configuration tools that encourage secure deployment across diverse environments.

7.3 MAC Randomization and Privacy Gaps

While MAC address randomization was introduced to mitigate tracking, most implementations still leak device identity through static probe behaviors, vendor-specific information elements, and predictable timing patterns. Future work should focus on developing enhanced randomization techniques that incorporate frame-level variability, temporal dynamics, and formal privacy models to strengthen resistance against correlation and re-identification attacks across diverse threat scenarios.

7.4 Underused RF Fingerprinting for Authentication

RF fingerprinting holds promise for device authentication based on unique radio emissions, but its adoption is limited due to environmental interference and the complexity of modeling physical layer features. Research should focus on developing lightweight and robust RF fingerprinting methods that are resilient to environmental variations, providing reliable authentication, particularly in IoT and resource-constrained environments.

7.5 WIDS in Noisy and Dynamic Environments

Conventional Wireless Intrusion Detection Systems (WIDS) face limitations in dynamic, mobile, or device-diverse environments, often producing high false positives or failing to detect novel threats. Advancing WIDS with adaptive machine learning models capable of real-time analysis, improved explainability, and reduced false alarm rates can significantly enhance threat detection in complex wireless ecosystems.

7.6 Unverified IEEE 802.11 Extensions

Recent IEEE 802.11 extensions such as Target Wake Time (TWT), Fast Initial Link Setup (FILS), and Wi-Fi Aware introduce new protocol logic, yet many of these features have not undergone formal security verification, leaving potential vulnerabilities undiscovered. Expanding formal modeling efforts to include modular and scalable analysis of these emerging amendments can support early-stage validation and improve the overall resilience of future Wi-Fi standards.

7.7 Security in Wi-Fi 6/6E/7 Evolution

Wi-Fi 6, 6E, and 7 introduce features like OFDMA, MU-MIMO, and higher modulation rates that enhance performance but also add protocol complexity and potential vulnerabilities. These upgrades may increase fingerprinting risk, complicate handshakes, and expose downgrade paths. Targeted security evaluations of these innovations are needed to uncover emerging threats and ensure that new capabilities do not compromise overall system resilience or compatibility.

7.8 Cross-Layer and Zero Trust Design

As Wi-Fi networks increasingly interface with cloud services and multi-device systems, traditional link-layer security alone is no longer sufficient. A shift toward cross-layer integration is needed to handle identity, access control, and data integrity holistically. Future Wi-Fi architectures should natively support cross-layer identity management, encrypted telemetry, and policy enforcement mechanisms consistent with enterprise-grade zero trust frameworks.

8 Conclusion

Wi-Fi has become central to modern communication across personal, enterprise, and industrial domains. Although the progression from WEP to WPA3 has strengthened wireless security, vulnerabilities such as KRACK, FragAttacks, and Dragonblood persist due to protocol complexity, legacy support, and evolving threats. This review highlighted ongoing challenges, including MAC tracking, device fingerprinting, and side-channel attacks, with particular concern in Industrial IoT (IIoT) deployments where low-power devices and outdated configurations amplify risk. We surveyed defense strategies including WPA3, WIDS, machine learning-based detection, and formal protocol verification. However, critical gaps remain in privacy preservation, real-time detection, and secure protocol rollout—especially as Wi-Fi 6, 6E, and 7 introduce new technical layers. Ensuring resilient Wi-Fi infrastructure demands a layered approach combining strong protocols, adaptive monitoring, and privacy-centric engineering. As wireless networks become foundational to digital infrastructure, continuous research and collaboration are essential for securing next-generation connectivity.

References

[1] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in *Proc. of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pp. 1313–1328, Oct. 2017.

[2] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," in *Proc. of the 2019 IEEE Symposium on Security and Privacy (S&P)*, pp. 517–533, May 2019.

[3] M. Vanhoef, "Fragment and Forge: Breaking WPA3, WPA2, and WEP Using Fragmentation and Aggregation Attacks," in *Proc. of USENIX Security Symposium*, 2021. [Online]. Available: https://www.fragattacks.com

[4] ESET Research, "Kr00k: Serious Vulnerability Affected Encryption of Over a Billion Wi-Fi Devices," ESET Whitepaper, Feb. 2020. [Online]. Available: https://www.welivesecurity.com/2020/02/26/kr00k-serious-vulnerability-affected-encryption-over-billion-wi-fi-devices

[5] Wi-Fi Alliance, "Wi-Fi Certified WPA3: Next Generation of Wi-Fi Security," Wi-Fi Alliance Whitepaper, 2018. [Online]. Available: https://www.wi-fi.org/discover-wi-fi/security

[6] J. Martin, D. Ye, and A. Juels, "A Study of MAC Address Randomization in Mobile Devices and When it Fails," in *Proc. of ACM WiSec*, pp. 45–56, July 2017.

[7] IEEE Std 802.11i-2004, "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 6: Medium Access Control (MAC) Security Enhancements," July 2004.

[8] B. Aboba, "IEEE 802.11i and TKIP," Microsoft Research, 2004. [Online]. Available: https://technet.microsoft.com/library/bb726942.aspx

[9] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," in *Proc. of IEEE Green Computing and Communications (GreenCom)*, pp. 21–26, Nov. 2016.

[10] R. Pang, M. Allman, M. Bennett, J. Lee, V. Paxson, and B. Tierney, "A First Look at Modern Enterprise Traffic," in *Proc. of ACM SIGCOMM Internet Measurement Conference (IMC)*, pp. 1–14, Oct. 2005.

[11] K. Kohbrok and D. J. Basin, "A Formal Analysis of 802.11's WPA2: Countermeasures for KRACK," in *Proc. of IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 316–

331, Apr. 2019.

[12] B. Blanchet, “Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif,” *Foundations and Trends in Privacy and Security*, vol. 1, no. 1–2, pp. 1–135, 2016.

[13] J. Wan, H. Yan, H. Suo, and F. Li, “Advances in Cyber-Physical Systems Research,” in *Proc. of IEEE ICSP*, pp. 1–6, Oct. 2011.

[14] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-Physical Systems Security—A Survey,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[15] M. Cunche, “I Know Your MAC Address: Targeted Tracking of Individual Using Wi-Fi,” *Journal of Computer Virology and Hacking Techniques*, vol. 10, no. 4, pp. 219–227, Nov. 2014.

[16] J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” in *Proc. of USENIX Security Symposium*, pp. 15–28, Aug. 2003.

[17] H. Mehboob, A. Javaid, and Z. Ali, “Intelligent Intrusion Detection System for IoT Networks Using Fuzzy Logic and Machine Learning,” in *Proc. of IEEE ICIOT*, pp. 10–16, Jul. 2020.

[18] D. Harkins, “Opportunistic Wireless Encryption (OWE),” IETF RFC 8110, Apr. 2017. [Online]. Available: https://tools.ietf.org/html/rfc8110

[19] NIST, “Zero Trust Architecture,” NIST Special Publication 800-207, Aug. 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207

[20] A. Lutu, M. Bagnulo, and J. Crowcroft, “On the Use of Wi-Fi in the Wild: The Case for Secure Wireless Connectivity in Public Spaces,” in *Proc. of ACM HotNets*, pp. 17–23, Nov. 2019.

[21] S. Hariharasitaraman and S. P. Balakannan, “A dynamic data security mechanism based on position aware Merkle tree for health rehabilitation services over cloud,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 1, pp. 1–15, Jul. 2019, Springer Berlin Heidelberg.