International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue5
Sep-Oct- 2026, PP 01-6

Wireless Network Security: A Review Of Threats, Security Protocols From Wep To Wpa3, And Ai-Assisted Intrusion Detection

Lokhande Sanghmitra Vinayak[1]; Prof. R. V. Varhade[2]; Prof. M. C. Kolse[3]; Prof. S. K. Said[4]
Department Of Artificial Intelligence And Data Science Jaihind College Of Engineering Pune, Maharashtra, India;

Abstract—Wireless technologies such as Wi-Fi, Bluetooth and mobile networks provide convenient connectivity without cables, but because signals travel through the air they are exposed to eavesdropping, unauthorized access, spoofing, denial-of-service and man-in-the-middle attacks. This paper reviews wireless network security. It analyses the main threats and traces the evolution of Wi-Fi security protocols: the cryptographic failures of Wired Equivalent Privacy, the improvements of Wi-Fi Protected Access and WPA2 with IEEE 802.11i, attacks such as key reinstallation that exposed flaws in WPA2's handshake, and the stronger but still scrutinized WPA3 with simultaneous authentication of equals. Weaknesses in Bluetooth key negotiation and in LTE link layers are also examined. Defensive measures, including strong passphrases, enterprise authentication with 802.1X, network segmentation, firewalls, firmware updates and wireless intrusion detection using machine learning on public datasets, are reviewed. A five-layer wireless security architecture comprising device hardening, secure association, encrypted transport, monitoring and incident response is proposed, along with research gaps, objectives, a comparison of protocols and challenges such as legacy devices, IoT constraints and user behaviour. The review concludes that layered defence with modern protocols and continuous monitoring is essential.

Index Terms—Wireless security, Wi-Fi, WEP, WPA2, WPA3, KRACK, Bluetooth security, wireless intrusion detection, 802.1X

I. Introduction

Homes, colleges, offices, cafés and railway stations all depend on wireless networks. Unlike a cable, a radio signal can be received by anyone nearby, so an attacker in the parking lot or the next room may capture traffic, impersonate an access point or jam the network. Zou *et al.* [1] surveyed wireless security and noted that the broadcast nature of the medium creates challenges distinct from wired networks.

Over two decades, Wi-Fi security has gone through several generations of protocols, each responding to attacks that broke the previous one. Bluetooth and cellular networks face their own vulnerabilities. Meanwhile, the number of wireless devices, including low-cost IoT gadgets, keeps growing.

This paper reviews wireless threats, the evolution of security protocols and modern defences including AI-assisted intrusion detection, and proposes a layered security architecture.

II. Background and Fundamental Concepts

2.1 Threats to Wireless Networks

Fig. 1 classifies threats into passive attacks (eavesdropping, traffic analysis) and active attacks (unauthorized access, rogue access points and evil twins, spoofing, man-in-the-middle, denial of service and jamming).

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue5
Sep-Oct- 2026, PP 01-6

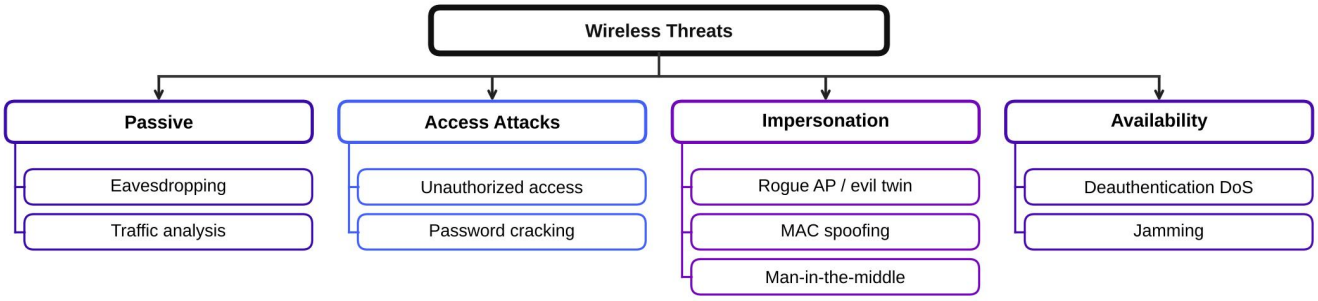


Fig. 1. Classification of wireless network threats.

2.2 Security Goals

Wireless security must provide confidentiality of data in the air, authentication of users and access points, integrity of frames and availability of the network.

III. Literature Survey

Borisov *et al.* [2] showed that WEP's design allowed attackers to decrypt and inject traffic because of short initialization vectors and a weak integrity check. Fluhrer *et al.* [3] revealed weaknesses in RC4's key scheduling that made WEP keys recoverable from captured traffic, leading to its deprecation. IEEE 802.11i [4] defined robust security networks with AES-based encryption and the four-way handshake used in WPA2.

Vanhoef and Piessens [5] discovered key reinstallation attacks (KRACK), in which an attacker manipulates handshake messages to force nonce reuse in WPA2, enabling decryption of traffic; vendors patched the flaw, but unpatched devices remain vulnerable. WPA3 [6] introduced simultaneous authentication of equals to resist offline password guessing, yet Vanhoef and Ronen [7] found side-channel and downgrade weaknesses in its early implementations (Dragonblood).

Bellardo and Savage [8] demonstrated practical denial-of-service attacks using spoofed deauthentication frames. Antonioli *et al.* [9] showed in the KNOB attack that Bluetooth key negotiation could be manipulated to use very short keys, and Rupprecht *et al.* [10] revealed LTE layer-two weaknesses allowing traffic redirection.

For detection, Kolias *et al.* [11] released the AWID dataset of real 802.11 traffic with attacks and evaluated machine learning detectors, finding that well-chosen features yield high detection rates. Table I summarizes these works.

TABLE I Summary of Literature Survey

Ref.	Author(s) / Year	Technique / Approach	Key Contribution	Limitation / Gap
[2]	Borisov et al., 2001	Analysis of WEP design	Showed decryption and injection	WEP-specific
[3]	Fluhrer et al., 2001	RC4 key-scheduling weakness	Enabled WEP key recovery	Cipher-level analysis
[8]	Bellardo and Savage, 2003	802.11 DoS attacks	Practical deauthentication attacks	Pre-PMF era
[11]	Kolias et al., 2016	AWID dataset and ML IDS	High detection with chosen features	Dataset ageing
[5]	Vanhoef and Piessens, 2017	KRACK attacks on WPA2	Forced nonce reuse	Patched on updated devices
[9]	Antonioli et al., 2019	KNOB Bluetooth attack	Low-entropy key negotiation	Bluetooth BR/EDR
[10]	Rupprecht et al., 2019	LTE layer-two attacks	Traffic redirection	Cellular only
[7]	Vanhoef and Ronen, 2020	Dragonblood WPA3 analysis	Side-channel and downgrade flaws	Early implementations

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue5
Sep-Oct- 2026, PP 01-6

IV. Research Gap

- 1. Many devices still use outdated protocols or default credentials.
- 2. Low-cost IoT devices often cannot support strong security or receive updates.
- 3. WPA3 adoption is incomplete, and transition modes can be downgraded.
- 4. Wireless intrusion detection datasets are limited and age quickly.
- 5. Users often choose weak passphrases or connect to untrusted public networks.

V. Objectives

- To analyse the threats facing wireless networks.
- To review the evolution and weaknesses of WEP, WPA, WPA2 and WPA3.
- To examine Bluetooth and cellular security issues.
- To propose a layered wireless security architecture with AI-assisted monitoring.
- To identify challenges and best practices.

VI. Proposed System Architecture

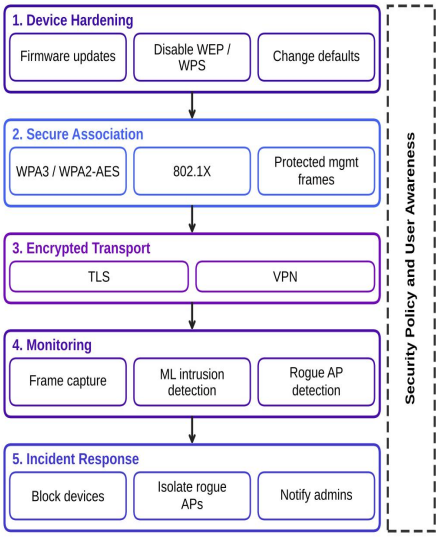


Fig. 2 shows the proposed architecture.

Fig. 2. Proposed layered wireless security architecture.

6.1 Device Hardening Layer

Access points and clients run current firmware, disable legacy protocols such as WEP and WPS, and change default credentials.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue5
Sep-Oct- 2026, PP 01-6

6.2 Secure Association Layer

Networks use WPA3 (or WPA2 with AES where WPA3 is unavailable); enterprises use 802.1X with individual credentials and protected management frames.

6.3 Encrypted Transport Layer

Application traffic is additionally protected with TLS [12] or VPNs, so that a compromised wireless link does not expose data.

6.4 Monitoring Layer

A wireless intrusion detection system captures management and data frames, extracts features and uses machine learning to detect deauthentication floods, rogue access points and abnormal behaviour.

6.5 Incident Response Layer

Alerts trigger blocking of offending devices, isolation of rogue access points and notification of administrators.

VII. Methodology and Working

Fig. 3 describes the monitoring workflow. A simple deauthentication-flood indicator counts deauthentication frames in a time window

$$r = N_deauth / \Delta t \quad (1)$$

and raises an alert when r exceeds a learned baseline. Machine learning classifiers trained on labelled frame features are evaluated with precision, recall and false-positive rate.

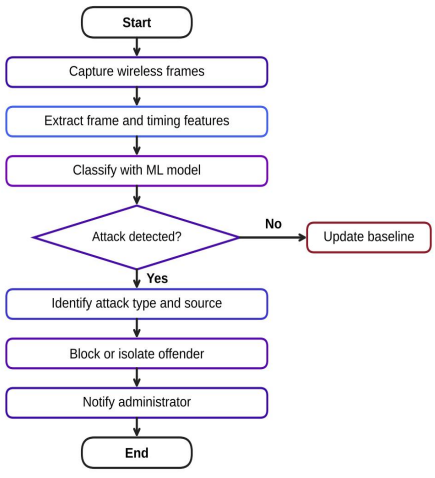


Fig. 3. Wireless intrusion monitoring workflow.

The strength of a passphrase against guessing grows with its entropy, so long passphrases are recommended even with WPA3.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue5
Sep-Oct- 2026, PP 01-6

VIII. Comparative Analysis

Table II compares Wi-Fi security protocols. WEP is broken, WPA with TKIP is deprecated, WPA2 with AES is acceptable when patched and WPA3 offers the strongest protection.

Protocol	Encryption	Authentication	Status
WEP	RC4 (weak IV)	Shared key	Broken
WPA	TKIP	PSK / 802.1X	Deprecated
WPA2	AES-CCMP	PSK / 802.1X	Acceptable if patched
WPA3	AES (GCMP option)	SAE / 802.1X	Recommended

TABLE II Comparison of Wi-Fi Security Protocols

IX. Challenges and Future Scope

Table III summarizes challenges. Future directions include broader WPA3 adoption, security for Wi-Fi 6 and 7 IoT devices, zero-trust network access, machine-learning detectors trained on current traffic and 5G network security.

Challenge	Mitigation
Legacy devices	Separate legacy SSID; replacement plan
IoT constraints	Network segmentation; IoT security standards
Weak passphrases	Long passphrases; enterprise auth
Rogue access points	Wireless IDS; certificate validation
Public Wi-Fi	VPN and HTTPS everywhere

TABLE III Challenges and Mitigation

X. Conclusion

Wireless convenience comes with security risks that have repeatedly surprised protocol designers. The reviewed literature traces how WEP failed, how WPA2 improved security but suffered KRACK, and how WPA3 strengthens authentication while still requiring careful implementation. Combining modern protocols, device hardening, end-to-end encryption and AI-assisted monitoring provides the layered defence that wireless networks need.

10.1 Acknowledgment

The authors express their sincere gratitude to the Department of Artificial Intelligence and Data Science, Jaihind College of Engineering, Pune, for providing the facilities, guidance and encouragement needed to carry out this work. The authors also thank the faculty members and colleagues whose valuable suggestions helped improve the quality of this review.

References

1. Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, 2016.
2. N. Borisov, I. Goldberg, and D. Wagner, “Intercepting mobile communications: The insecurity of 802.11,” in Proc. 7th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom), 2001, pp. 180–189.

3. S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” in Proc. Sel. Areas Cryptogr. (SAC), 2001, pp. 1–24.
4. IEEE Standard for Information Technology—Part 11: Wireless LAN MAC and PHY Specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11i-2004, 2004.
5. M. Vanhoef and F. Piessens, “Key reinstallation attacks: Forcing nonce reuse in WPA2,” in Proc. ACM CCS, 2017, pp. 1313–1328.
6. Wi-Fi Alliance, “WPA3 Specification,” Version 1.0, 2018.
7. M. Vanhoef and E. Ronen, “Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd,” in Proc. IEEE Symp. Security Privacy, 2020, pp. 517–533.
8. J. Bellardo and S. Savage, “802.11 denial-of-service attacks: Real vulnerabilities and practical solutions,” in Proc. 12th USENIX Security Symp., 2003.
9. D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, “The KNOB is broken: Exploiting low entropy in the encryption key negotiation of Bluetooth BR/EDR,” in Proc. 28th USENIX Security Symp., 2019, pp. 1047–1061.
10. D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, “Breaking LTE on layer two,” in Proc. IEEE Symp. Security Privacy, 2019, pp. 1121–1136.
11. C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, “Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset,” IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 184–208, 2016.
12. E. Rescorla, “The Transport Layer Security (TLS) protocol version 1.3,” IETF RFC 8446, 2018.