International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 928-929
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0133

WI-FI Jammer Simulator & Mitigation System

Dr. S Lavanya [1], Abaka Jayakumar[2], Karthikeyan V[3], Prakash R[4]
[1]Associate Professor and HOD Department of CSE Sri Ranganathar Institute of Engineering and Technology Coimbatore, India
[2,3,4]UG - Department of CSE, Sri Ranganathar Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India
Emails: *lavanya@sriet.ac.in[1], jayakumarabaka@gmail.com[2], karthivvadivel62@gmail.com[3], praramesh2003@gmail.com[4]*

Abstract
Wi-Fi networks are widely used in homes, enterprises, and IoT systems due to their convenience and low deployment cost. However, they are vulnerable to attacks such as deauthentication and jamming, which disrupt availability and disconnect legitimate users. This project presents a Wi-Fi Jammer Simulator & Mitigation System designed purely for academic and educational purposes. Instead of performing illegal jamming, the system simulates attack conditions in a controlled environment to demonstrate how disruptions occur and how recovery mechanisms work. The system detects abnormal Wi-Fi behavior such as sudden disconnections, signal drops, and packet loss, and applies mitigation techniques including automatic reconnection and channel switching. A web-based dashboard visualizes attack detection, system status, and mitigation results in real time. The project emphasizes ethical experimentation and aims to educate students on wireless network vulnerabilities and resilience strategies.
Keywords: Wi-Fi Security, Jammer Simulation, Deauthentication Attack, Mitigation Techniques, Network Monitoring, Ethical Hacking.

1. Introduction
Wireless networks have become an essential part of modern communication systems. Wi-Fi technology enables seamless internet access for laptops, smartphones, smart home devices, and industrial IoT applications. Despite its widespread adoption, Wi-Fi networks are vulnerable to several security threats that can affect availability, confidentiality, and integrity. One of the most common threats is the deauthentication attack, which can be exploited to disconnect users from a network without their consent. The Wi-Fi Jammer Simulator & Mitigation System focuses on simulating jamming behavior rather than executing actual illegal attacks. The goal is to demonstrate detection and recovery logic through software-based simulation and visualization. By leveraging monitoring modules and dashboards, the system provides a safe and ethical platform for students to understand Wi-Fi security threats and resilience mechanisms. This project also aims to bridge the gap between theoretical knowledge and practical implementation in the field of wireless network security. [1-5]

2. Methods
The system architecture consists of several modules: attack simulation, detection logic, mitigation engine, and visualization dashboard. The attack simulation module mimics real-world Wi-Fi jamming and deauthentication scenarios by introducing artificial disconnections and signal degradation. The detection logic continuously monitors Wi-Fi parameters such as signal strength, packet loss, and connection status. Threshold-based rules are used to identify abnormal behavior indicative of an attack. Once an attack is detected, the mitigation engine attempts to restore connectivity by switching channels or re-establishing the connection. All events and actions are logged and visualized in a web-based dashboard, which provides real-time feedback to the user. The system is implemented using Python and JavaScript, with backend support for data logging and frontend

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 928-929
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0133

visualization using web technologies.

3. Experimental Input Parameters

Table 1 Input Parameters

Parameter	Normal Condition	Simulated Attack
Signal Strength (dBm)	-50	-90
Packet Loss (%)	1	40
Disconnection Events	0	5

4. Figures

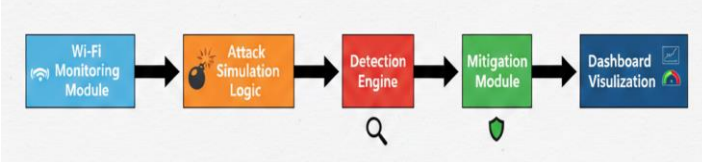

Figure 1 Flow Chart

5. Results and Discussion

The system was tested under various simulated attack conditions. During the tests, the simulator successfully induced Wi-Fi disconnections and signal degradation. The detection module accurately identified these anomalies based on predefined thresholds. The mitigation engine responded promptly by attempting reconnections and switching to alternative channels, which restored connectivity in most cases. The dashboard provided a clear and intuitive interface for monitoring system status. It displayed real-time graphs of signal strength, packet loss, and disconnection events. This visualization helped users understand the impact of attacks and the effectiveness of mitigation strategies. The results demonstrate the potential of the system as an educational tool for teaching wireless security concepts.

Conclusion

This project presents an educational Wi-Fi Jammer Simulator & Mitigation System that helps students understand Wi-Fi security threats and recovery mechanisms. By focusing on simulation rather than real attacks, the system ensures ethical use while delivering practical insights into network resilience and security concepts. Future enhancements may include machine learning-based anomaly detection, support for multiple access points, and integration with enterprise-grade monitoring tools. [6-10]

Acknowledgements

We would like to thank our guide and team members for their support and contributions to this project.

References

[1]. [1] IEEE Std 802.11™, “IEEE Standard for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” IEEE, 2020.

[2]. [2] M. Gast, “802.11 Wireless Networks: The Definitive Guide,” 2nd ed., O’Reilly Media, 2005.

[3]. J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” in Proc. 12th USENIX Security Symposium, 2003, pp. 15–28.

[4]. K. Bicakci and B. Tavli, “Denial-of-Service Attacks and Countermeasures in IEEE 802.11 Wireless Networks,” Computer Standards & Interfaces, vol. 31, no. 5, pp. 931–941, 2009.

[5]. S. Khan, M. Imran, and M. Shoaib, “Detection of Wi-Fi Deauthentication Attacks Using Network Traffic Analysis,”

[6]. International Journal of Computer Networks & Communications, vol. 10, no. 3, pp. 1–12, 2018.

[7]. A. Mishra and W. Arbaugh, “An Initial Security Analysis of the IEEE 802.11 Protocol,” University of Maryland, Technical Report, 2002.

[8]. Cisco Systems, “Wireless LAN Security Best Practices,” White Paper, Cisco, 2021.

[9]. Wireshark Foundation, “Wireshark User Guide and Network Traffic Analysis,” 2020. [Online].Available:https://www.wireshark.org

[10]. S. Haykin, “Communication Systems,” 4th ed., Wiley India, 2008.

[11]. N. Behl and J. Behl, “Cyberwarfare: Security, Strategy, and Practice,” Oxford University Press, 2017.