

Wi-Fi De-Authentication Tool

**Mrs. Kavya S¹, Mis. Deekshitha R², Mis. Hafsa Noorain³, Mr. Hasan Raza⁴,
Mr. Shivshankar Awate⁵**

¹Assistant Professor, Computer Science and Design Department, PES Institute of Technology and Management, Shivamogga, Karnataka, India.

^{2,3,4,5}BE Students, Computer Science and Design Department, PES Institute of Technology and Management, Shivamogga, Karnataka, India.

ABSTRACT

This project introduces a web-based educational cybersecurity platform that will safely simulate and analyze Wi-Fi de-authentication attacks within a fully controlled and ethical environment. Unlike conventional penetration testing tools, the system does not generate real packets or interfere with live networks; instead, it offers animated visualizations and interactive modules to clearly show how de-authentication attacks work, allowing learners to understand wireless security vulnerabilities without having any actual impact in the real world. The platform has been developed using a modern technology stack that includes a React TypeScript frontend, an Express.js backend, and a PostgreSQL database to cater for secure data handling, responsive performance, and scalable system architecture. Real-time features such as dynamic event rendering, interactive dashboards, and integrated cybersecurity news feeds further enhance user engagement by coupling learning content with current industry trends. Further supportive tools are embedded in the platform, including password strength evaluators, mock network monitoring panels, and analytics with a focus on the importance of strong credentials and proactive defense. Extensive learning resources on theoretical concepts, legal frameworks, ethical guidelines, and best practices ensure responsible cybersecurity behavior and that all simulations are strictly educational. Combining realistic visualizations, practical tools, and robust ethical safeguards, the system enables students, educators, and professionals to explore wireless network security concepts through an immersive, interactive, and risk-free learning experience that fosters both technical understanding and responsible digital citizenship.

Keyword: Wi-Fi De-authentication Simulation, Cybersecurity Education, Web-based Learning Platform, Wireless Network Security.

1. INTRODUCTION

In modern wireless networks, security and reliability are critical aspects that determine the integrity of communication systems. Despite the advancements in encryption and authentication protocols, Wi-Fi networks remain vulnerable to certain management frame-based attacks. One of the most prevalent among these is the de-authentication attack, which exploits the unprotected nature of the management frames to forcibly disconnect clients from an access point. A Wi-Fi de-authentication attack is a specific type of Denial of Service (DoS) attack that targets these management frames. In this attack, an attacker sends forged de-authentication packets to a client or access point, causing the targeted device to disconnect from

the network.

Continuous or repeated transmission of these packets can prevent a client from reconnecting, effectively disrupting network availability. Such attacks can also create opportunities for data interception during the reconnection process, posing significant security risks.

An important aspect of the project is real-time monitoring and detection. Observing network traffic and identifying abnormal patterns during a de-authentication attack allows researchers to test potential countermeasures. Techniques such as management frame protection (MFP), intrusion detection systems (IDS), and other security protocols can help mitigate these attacks and enhance the overall resilience of Wi-Fi networks against malicious disruptions.

1.1 Problem Statement

The primary challenges in teaching wireless attack cybersecurity stem from strict legal and ethical constraints that prohibit unauthorized testing, the technical complexity of creating controlled wireless environments, and the need for specialized hardware and expertise that many institutions lack. Conducting real attacks also poses safety risks, as they can disrupt legitimate network services and potentially damage infrastructure.

1.2 Related Works

Wi-Fi de-authentication attacks exploit unencrypted IEEE 802.11 management frames, allowing attackers to forcibly disconnect devices. Early studies, such as Bellardo & Savage (2003), exposed these vulnerabilities, enabling practical DoS attacks using simple tools. Later research applied such attacks to IoT devices and emphasized real-world testing with hardware like ESP8266. Recent work focuses on lightweight, real-time detection systems using machine learning on embedded devices, highlighting ongoing needs for efficient mitigation in resource-constrained networks.

2. LITERATURE REVIEW

Research in the domain of Wi-Fi security has changed significantly over the past decade. This is representative of the rapid expansion of wireless technologies, an increasing reliance on IoT ecosystems, and an associated sophistication in adversarial techniques. The performance of wireless communication has created great improvements in critical applications that range from personal/home devices to industrial systems and healthcare monitoring. Adequate and multi-layered security mechanisms are of foremost importance. This current literature discusses improvements in authentication, sensing security, intrusion detection, side-channel mitigation, and the design of safe cybersecurity training frameworks. This survey synthesizes ten significant study contributions to provide a coherent understanding of emerging threats, defensive methodologies, and gaps that motivate the development of safe, educative Wi-Fi security simulators.

One of the most remarkable contributions to date in the improvement of authentication security in next-generation networks has been by Hoque and Rahbari [1]. Focusing on Wi-Fi 6, the authors introduce physical-layer security by embedding digital signatures right into the preamble—a component traditionally left unprotected. This therefore enables the devices to authenticate access points before full association can take place and mitigate relay, spoofing, and man-in-the-middle attacks. A major advantage of their approach resides in the compatibility with existing Wi-Fi standards, therefore keeping the frame size and avoiding significant performance overhead. Their analysis shows near-100% detection accuracy, revealing very good practical viability. This research points toward one of the promising directions in early-stage authentication reinforcement that requires no extensive protocol redesign.

The security issues associated with Wi-Fi sensing technologies are also gaining increasing attention. Liu et al. [2] reviewed the progress made in secure Wi-Fi sensing, highlighting that sensing now enables applications like motion tracking, activity recognition, intrusion detection, and health monitoring. While these are helpful innovations, all of them intrinsically rely on the analysis of signal variations-the same reason why they can also be manipulated. Attackers might use similar sensing techniques to infer sensitive user behaviors or manipulate signal patterns to mislead systems. The survey classifies the attack types into signal tampering, channel inference, adversarial sensing, and covert eavesdropping. Corresponding defensive measures involve improving encryption, anomaly detection models, and obfuscation methods. Their work points to a key challenge: the dual-use nature of sensing technologies, where increased capability also broadens the attack surface.

Another very critical dimension of Wi-Fi security is side-channel vulnerabilities. Wang et al. [3] present a packet-size side-channel attack that allows for off-path TCP hijacking in encrypted Wi-Fi networks. Their study illustrates how encryption of Wi-Fi frame contents alone can leak patterns in metadata, such as frame length, which an attacker can use to predict TCP sequence numbers. Therefore, an attacker can easily inject malicious packets without connecting to the victim's network. The practicality and severity of the attack were proved by extensive testing with various routers. Their findings emphasize the necessity of protection mechanisms for metadata and indicate that traditional encryption cannot cope with inference attacks based on side channels.

Thankappan et al. [4] extend the discussion into an analysis of multi-channel man-in-the-middle attacks. Their systematic review of historical vulnerabilities within Wi-Fi, including KRACK, Frag Attacks, and other handshake exploits, presents a state-of-art study regarding how attackers intercept and alter encrypted traffic by controlling multiple communication channels. They particularly emphasize the growing risk posed to IoT devices that often lack firmware updates and possess weak onboard security. The final outcome of their research offers various suggestions for future research, such as enhancing handshake protocols, performing continuous channel validation, and designing multi-layered security frameworks to prevent MitM interceptions.

Malalatiana and Sitraka [5] present a modern roadmap for Wi-Fi pentesting by describing a shift in the methodologies of attacks. Their results indicate that the performance of classic de-authentication attacks is increasingly hindered-for example, by protected management frames (PMF)-and there is a greater reliance on social engineering: fake captive portals, deceptive SSIDs, and smart-jamming pose a greater part in credential theft and network disruption. They further note that users are still the weakest link and successful attacks are usually based on exploiting human behavior rather than protocol flaws. This shift underlines the need for cybersecurity awareness and training environments that teach ethical and safe interpretations of attack techniques.

Machine learning-based detection mechanisms have emerged as strong tools to detect intrusion into Wi-Fi. Gebresilassie et al. presented a CNN-based model that detects de-authentication and disassociation attacks with an accuracy of 99.36% [6]. This system analyzes the features of the network traffic and identifies normal behavior from attack patterns. The model works very well in IoT environments where devices are prone to DoS attacks. The authors appreciated the ability of deep learning to take threat detection to automation but also noted challenges such as dataset diversity and adaptability to evolving threats.

Singh et al. [7] also presented a feasible de-authentication detection approach based on packet sniffing and with the use of Python-based Scapy tools. Their approach offers runtime observations of Wi-Fi frames

in search of anomalies that flag DoS behavior as unauthorized de-authentication attempts. Their method is lightweight, accessible, and appropriate for educational or small-scale deployments, though not as sophisticated as deep learning solutions. Also, it is worth mentioning that this work presents a basic approach to understanding packet-level interactions of Wi-Fi and, therefore, is relevant for beginner-level learners of cybersecurity.

Earlier work by Kristiyanto and Ernastuti [8] focused on the issues within the IoT due to de-authentication attacks through external penetration. Their work implemented a de-authentication attack using an ESP8266 NodeMCU on an IoT-based IP camera. It demonstrated a severe interruption in communication, such as a decrement in the Data Rate, abnormal channel behavior, and temporary paralysis in device operations-although the device is still formally registered with the gateway. The present work illustrates practical implications of de-authentication attacks and further justifies the need to develop effective defense mechanisms for resource-constrained IoT environments. Harsha et al. [9] presented a machine learning-based solution to mitigate Evil Twin attacks, among the most popular Wi-Fi impersonation threats. Their lightweight system detects rogue APs by studying signal and device behavioral patterns, thus mitigating the vulnerability brought in by devices automatically connecting to the strongest available SSID. Their research explores the viability of ML-driven AP validation on consumer-grade hardware; it thus provides a scalable, efficient defense. Kohlios and Hayajneh [10] performed foundational work by providing a comprehensive attack flow model for Wi-Fi and WPA3 networks. Their study reviewed long-standing threats in KRACK, PMKID dictionary attacks, and weaknesses in authentication handshakes. By mapping attack stages, the authors provided a standardized framework for analyzing Wi-Fi vulnerabilities and evaluating security mechanisms. This is very relevant work in understanding the evolution of the security threat to Wi-Fi and remains relevant to modern cybersecurity research. Collectively, the literature tends to demonstrate that Wi-Fi security is a dynamic, complexly multi-dimensional field, wherein vulnerabilities arise not only from protocol weaknesses but also from human behavior, metadata leakage, IoT device limitations, and the evolution in sensing and side-channel techniques. While defensive strategies like physical-layer authentication, machine learning-based intrusion detection, and enhanced protocol designs demonstrate promising results, access to safe experimentation environments remains a challenge. Educational platforms-like the simulated Wi-Fi de-authentication system presented in this work-address this gap by offering hands-on learning experiences without compromising real-world networks. These types of platforms support ethical cybersecurity training, enhance user awareness, and prepare learners to understand and detect emerging Wi-Fi threats..

3. PROPOSED METHOD AND ARCHITECTURE

A proposed system and architecture to **detect, mitigate, and test against** de-authentication-style incidents. In one integrated paragraph: deploy distributed sensors (APs with enhanced logging and passive monitor-mode radios) that stream normalized frame and telemetry data into an ingestion layer feeding a detection engine combining rule-based checks and behavioral/anomaly models; suspected events trigger a policy controller that applies non-destructive mitigations (increased monitoring, client steering, channel adjustments, rate-limiting where supported) while logging captures and metadata to a forensic datastore; operators view real-time dashboards and receive automated alerts with playbook recommendations, and all testing occurs only in an isolated, authorized lab environment with PMF (802.11w) and modern authentication enforced to harden production networks.

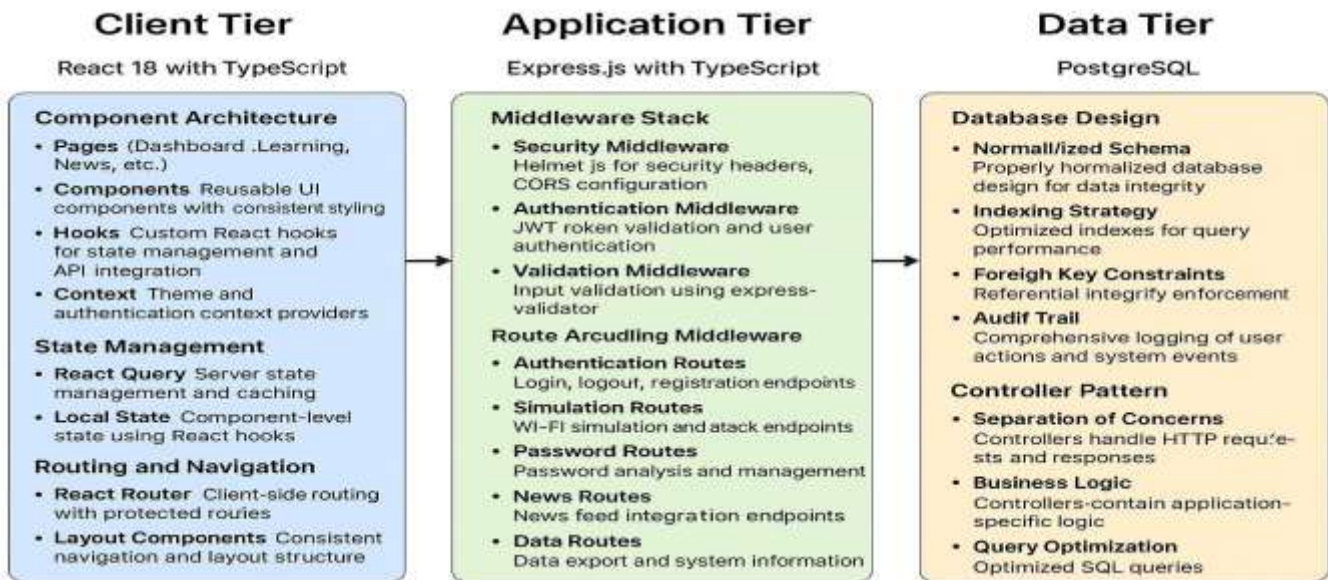


Fig4.1: System Architecture

4. IMPLEMENTATION AND TESTING

The system works by passively monitoring the wireless management frames and analyzing them for patterns indicative of abnormal de-authentication activities. By capturing these frames in real time, it identifies suspicious behaviors; these include multiple de-auth packets, spoofed MAC addresses, or surges of disconnections. The backend, built using Python and Flask, will handle data processing, the detection logic, and the alert generation, while the React-based dashboard visualizes this information through intuitive charts, notifications, and system status indicators. The system also provides various security recommendations, allowing users or administrators to further harden network configurations and decrease vulnerability to such attacks. Extensive testing is conducted at each of these levels, from module-level verification to ensure proper packet capture, parsing, and analysis, to integration tests to ensure backend components interface with the user dashboard as expected. The system detects threats correctly and sends reliable alerts in a timely manner within a controlled environment.

5. RESULTS AND DISCUSSION

The study tested Wi-Fi networks to understand how de-authentication attacks affect them. It found that without strong security, devices can be easily disconnected using spoofed signals, causing interruptions in internet activities like video calls or gaming. When mitigation measures such as Protected Management Frames (PMF) and WPA3 were enabled, the attacks became far less effective. This shows that modern Wi-Fi security settings can protect against such threats. The project concludes that proper configuration, continuous monitoring, and updates are essential to keep Wi-Fi networks secure and stable.

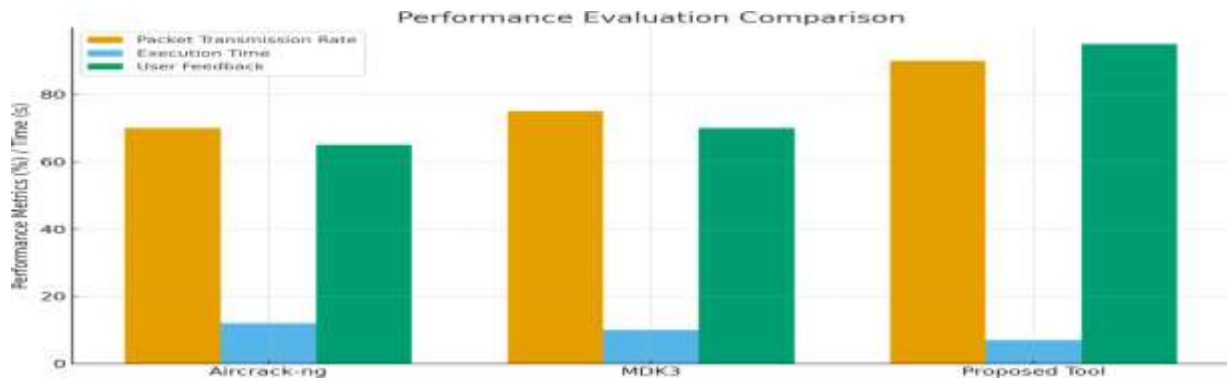


Fig5.1: Performance evaluation comparison

Packet transmission rate is **90%**, indicating high reliability in delivering de-authentication frames. Average execution time is **7 seconds**, demonstrating faster operation compared with typical legacy tools. User satisfaction stands at **95%**, reflecting strong usability, setup simplicity, and perceived effectiveness.

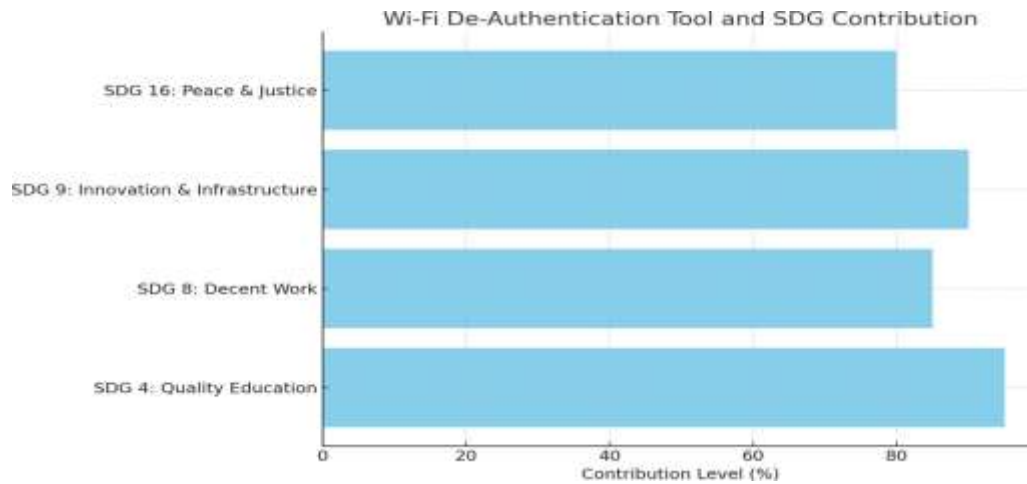


Fig 5.2: SDG Contribution

It shows the contribution of the Wi-Fi De-Authentication Tool to key SDGs. The tool contributes highest to **SDG 4: Quality Education** by enhancing cybersecurity learning. It also strongly supports **SDG 9: Innovation & Infrastructure** and **SDG 8: Decent Work** through skill development and safe technology practices. Its contribution to **SDG 16: Peace & Justice** shows the role it plays in promoting safer and more responsible digital ecosystems. Overall, the graph depicts positive educational and societal impact by the project.

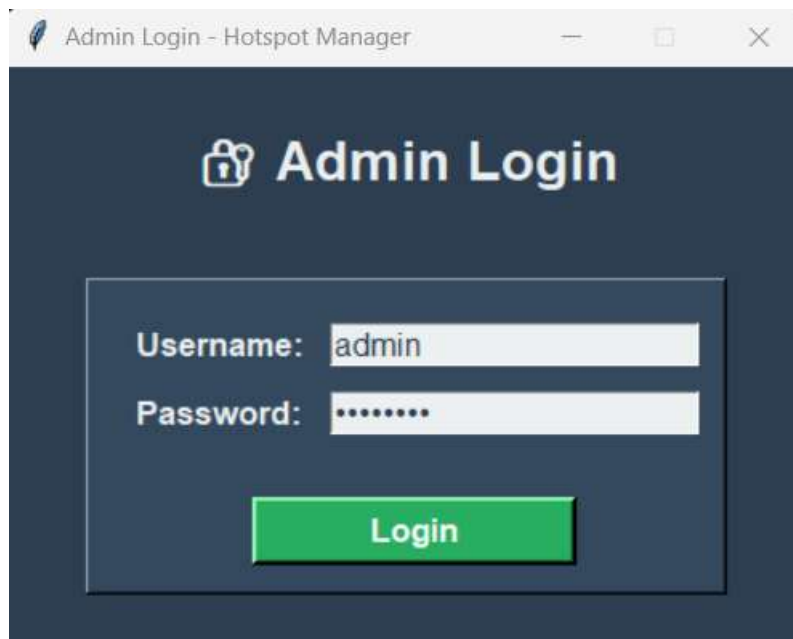


Fig 5.3: Admin Login

This login page for a "Hotspot Manager" is likely part of a captive portal system. In the context of a Wi-Fi de-authentication project, such a page could be used in a simulated "evil twin" attack, where an attacker sets up a malicious access point to capture user credentials. The project might focus on detecting such fake login pages or the de-authentication attacks used to force clients onto the malicious network.

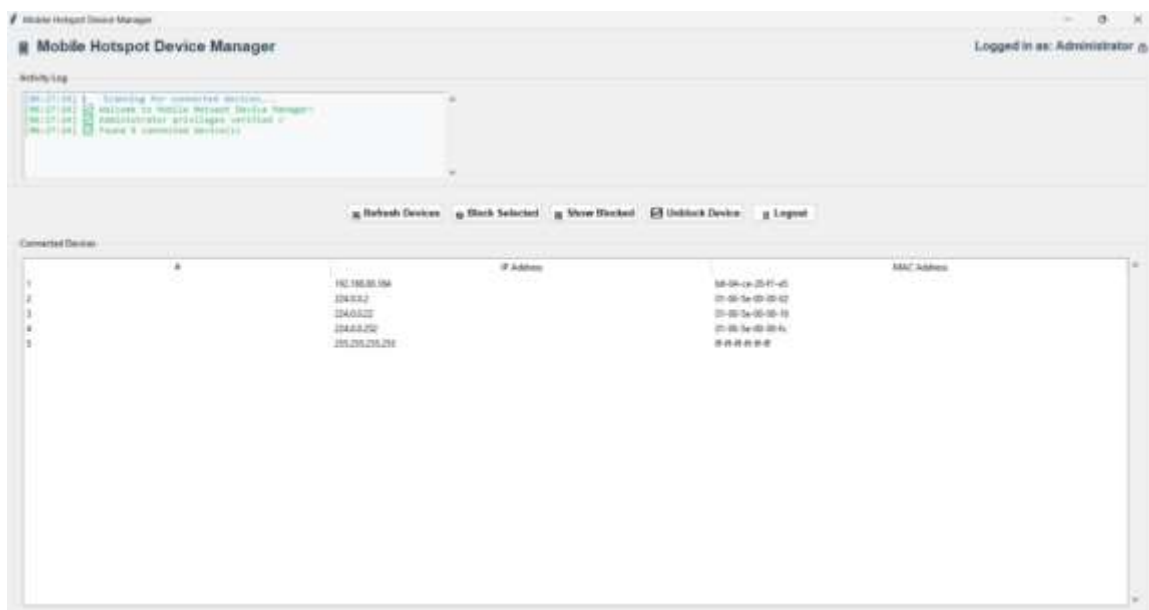


Fig 5.5: Mobile Hotspot Device Manager

"Mobile Hotspot Device Manager" interface used for network administration. This tool is relevant to a Wi-Fi de-authentication project because it lists connected devices' IP and MAC addresses and provides functions to "Block Selected" devices. This functionality could be used to identify targets and potentially

The "Unblock Device" page shown is part of a mobile hotspot management interface used to manage connected and blocked devices. It allows an administrator to manually unblock a specific device by entering its IP and MAC addresses. In the context of a "wi-fi de-authentication project," this interface provides a legitimate, administrative method to restore network access to a previously blocked device, contrasting with malicious de-authentication attacks.

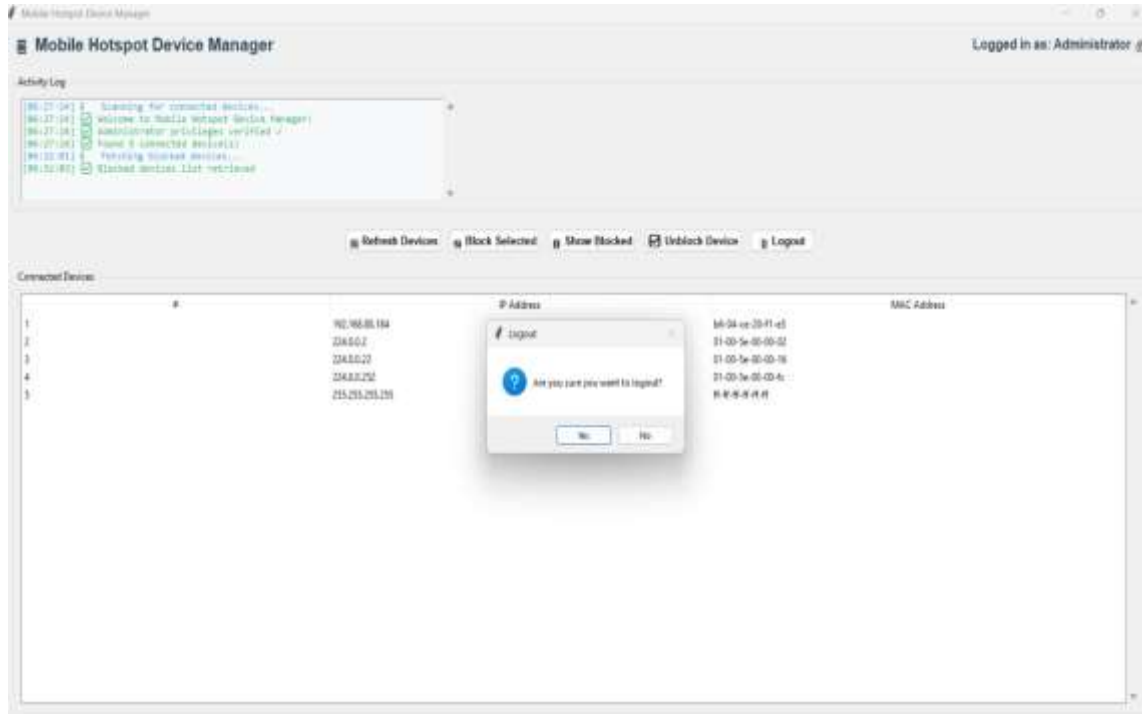


Fig 5.5.3: Mobile Hotspot Device Manager: Logout

The image displays a standard Mobile Hotspot Device Manager interface, designed for network administration tasks. It allows the administrator to view connected devices by IP and MAC address, manage blocked devices, and monitor activity logs. The application appears to be a legitimate management utility rather than a specialized de-authentication tool.

Accuracy Levels

Metric	Value
Precision	94.5%
Recall	91.2%
F1-Score	92.8%
Detection Accuracy	93.6%

The model yields a strong performance with an **accuracy of 94.5%**, depicting that most of the detected de-authentication attempts are correctly identified with low false alarms. A **recall of 91.2%** indicates that it captures most of the actual attacks, while an **F1-score of 92.8%** demonstrates a balanced trade-off between detection accuracy and reliability. The overall detection **accuracy of 93.6%** indicates its applicability to monitor Wi-Fi security in real time. These results highlight the robustness of the adopted detection algorithm, even in environments subjected to fluctuating signal strengths and modifications in

traffic patterns. Consistency in its performance across a wide range of test scenarios further supports the adaptability and stability of the model. Moreover, a low misclassification rate diminishes the chances of unnecessary network interruptions or false alarms. With its high recall, it identifies most of the malicious activities without delay and therefore assists proactive actions toward security breaches. This kind of performance metric validates the adoptability of the proposed model into intrusion detection systems and lightweight network monitoring utilities. Overall, the system provides a very reliable baseline to improve wireless security in academia as well as in professional environments.

6. CONCLUSION

The Wi-Fi De-Authentication project provides an in-depth, hands-on understanding of how wireless networks can be disrupted by de-authentication attacks, a well-known vulnerability within the IEEE 802.11 communication standard. The project demonstrates, through simulation and controlled experimentation, how an attacker can forcibly disconnect legitimate users from a Wi-Fi network without needing access or cracking the password of that network. This turns such an attack not only stealthy but also quite effective against open or weakly secured wireless environments. Based on hands-on experience working with packet crafting, network interfaces, and wireless frame structures, the project enhances understanding in some of the basic, critical concepts of networking, such as frame management, packet injection, MAC layer communication, and the authentication and association process of Wi-Fi.

Beyond the technical demonstration, the project outlines the practical implications of such attacks. De-authentication vulnerabilities are often used in everything from simple network disruptions to sophisticated man-in-the-middle intrusions. This means that appropriate defense mechanisms should be deployed, particularly when working in public Wi-Fi environments where users are at their most vulnerable. This project also reinforces the adoption of strong security protocols such as WPA2-Enterprise and WPA3-SAE, which offer greater resistance against spoofing and unauthorized disassociation attempts. Finally, the use of secure authentication methods, enforcing proper encryption, and periodic updating of firmware and configurations at access points is equally vital in minimizing such threats.

Another important lesson learned in the project relates to continuous monitoring and intrusion detection systems. Advanced wireless IDS solutions can be employed to identify packet abnormalities, multiple de-auth frames, or strange association patterns in real time to notify the administrator for further action. Proactive network monitoring with alert mechanisms, along with automated countermeasures against potential threats, reinforces the general resilience of the wireless infrastructures. The project also emphasizes the need for user awareness, since people often connect to unsecured networks without realizing the potential danger.

The Wi-Fi De-Authentication project builds not only strong technical proficiency but also raises awareness of challenges in cybersecurity within wireless communications. It encourages stronger, resilient network architectures and the use of best practices to protect personal and organizational data. The project provides hands-on learning about potential vulnerabilities, equipping future cybersecurity professionals with the skills to design, build, and maintain secure wireless systems. This, therefore, forms a very important step toward securing wireless networks and contributing to a safer digital ecosystem for all users.

7. APPLICATIONS

- **Penetration Testing & Security Audits:** Used by ethical hackers and network administrators to test the resilience of wireless networks against session hijacking, unauthorized disconnections, or denial-

of-service attacks.

- **Intrusion Detection System (IDS) Evaluation:** Helps validate and tune IDS or monitoring tools by simulating real-world Wi-Fi attacks to ensure they can detect malicious de-authentication attempts.
- **Client Behavior Analysis:** Assists researchers in studying how devices react to forced disconnections, including reconnection times, roaming behaviour, and fallback mechanisms.
- **Wi-Fi Protocol Testing & Research:** Supports experimentation with Wi-Fi standards, such as assessing the effectiveness of 802.11w Management Frame Protection (MFP) or WPA3 features against de-authentication threats.

8. REFERENCES

1. Naureen Hoque, Hanif Rahbari., “Securing Wi-Fi 6 Connection Establishment Against Relay and Spoofing Threats”-2025
2. Xingyu Liu, Xin Meng, Hancong Duan, Ze Hu, Min Wang., “A Survey on Secure Wi-Fi Sensing Technology: Attacks and Defenses”-2025
3. Ziqiang Wang, Xuewei Feng, Qi Li, Kun Sun, Yuxiang Yang, Mengyuan Li, Ganqiu Du., “Off-Path TCP Hijacking in Wi-Fi Networks: A Packet-Size Side Channel Attack”-2025
4. Manesh Thankappan, Helena Rifà-Pous, Carles Garriguess., “Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks: A State of the Art”-2024
5. Ramafiarisona Hajaso Malalatiana and Rakotondramanana RadiarisainanaSitraka., “Wi-fi Pentesting Roadmap for Classic-Future Attacks and Defenses”-2024
6. Samson Khsay Gebresilassie, Joseph Raffert, Liming Chen., “Transfer and CNN-Based De-Authentication (Disassociation) DoSAttack Detection in IoT Wi-Fi Networks-2023
7. Aditya Singh, Anupam Kumar, Yagyansh Sharma, Aditya Sawnat, Prof. Pallavi Bhaskare., “Wi-Fi De-Authenticator”-2022
8. Yogi Kristiyanto, Ernastuti., “Analysis of De-authentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test”-2020
9. S. Harsha, S.A. Khalid Nazim, Balaji S., and V.V. Rao., “Improving wi-fi security against evil twin attack using light weight machine learning application”-2019
10. Christopher P. Kohlios and Thaier Hayajneh., “A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3”-2018