IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121019

WiFi Deauthentication Device for Ethical Hacking and Security Testing

Mr. VIKRAM P[1], MOHAMED FAIZE A[2], THIRUVIKRAM S[3], KABILAN M[4]

Assistant Professor, Department of IT, Kongunadu College of Engineering and Technology, Tamil Nadu, India[1]

Department of IT, Kongunadu College of Engineering and Technology, Tamil Nadu, India[2-4]

Abstract: Wireless networks are increasingly vulnerable to attacks that exploit weaknesses in the IEEE 802.11 protocol, particularly through the misuse of unencrypted management frames. One such attack is the WiFi deauthentication attack, which forcibly disconnects clients from access points by sending forged deauth packets. This project presents the design and implementation of a portable WiFi deauthentication device using the ESP8266 microcontroller, an SSD1306 OLED display, and button-based navigation.The device enables users to scan nearby WiFi networks, select targets, and initiate deauthentication attacks in a controlled and ethical environment. It serves as a practical tool for security researchers, ethical hackers, and educators to demonstrate wireless vulnerabilities and promote awareness of network security best practices. The system is fully standalone, requiring no external computer or software, and is built using open-source libraries and firmware.

Keywords: “WiFi Deauthentication, ESP8266, Ethical Hacking, Wireless Security, 802.11 Protocol".

I. INTRODUCTION

In the evolving landscape of cybersecurity, wireless networks remain a critical yet vulnerable component of modern digital infrastructure. Among the various attack vectors targeting WiFi systems, deauthentication attacks have emerged as a simple yet powerful method to disrupt connectivity and exploit network weaknesses. These attacks exploit the 802.11 protocol by sending forged deauthentication frames, forcing devices to disconnect from access points without proper authorization.While malicious actors have long used deauthentication techniques for denial-of-service (DoS) or man-in-the-middle (MITM) attacks, ethical hackers and security researchers now leverage these same tools to test network resilience, identify vulnerabilities, and develop robust countermeasures. Devices such as the ESP8266, NodeMCU, and Linux-based WiFi adapters have become popular platforms for simulating these attacks in controlled environments due to their affordability, portability, and programmability.

II. SYSTEM ARCHITECTURE

Packet Sniffing Module

This module is responsible for capturing all WiFi packets in the surrounding environment by setting the ESP8266 microcontroller into promiscuous mode. By intercepting and analyzing 802.11 management frames—particularly deauthentication packets—the device can monitor the wireless spectrum for both standard and malicious activities. This serves as the foundational layer that enables subsequent detection and attack functionalities. The module is validated using tools such as Wireshark and verified with Arduino IDE serial outputs.

DEAUTHENTICATION ATTACK MODULE

Once a target has been identified, this module constructs and sends forged deauthentication frames to the selected client or access point. The ESP8266’s native packet injection capabilities are harnessed, allowing the device to disrupt client connections by transmitting crafted packets that comply with WiFi standards. This simulates a real-world deauthentication attack, providing users with an authentic demonstration of the vulnerability. The module accepts user-defined MAC addresses and supports configurable attack intervals.

Network Scanning Module

This module systematically scans all available WiFi networks and discovers connected clients within the vicinity. Using ESP8266 SDK functions, the module lists SSIDs and associated devices, presenting the detected data on the

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121019

OLED display. This real-time scanning enables users to select valid targets easily and ensures a broad awareness of the wireless landscape around the device.

Central processing unit controlling the display and reading user inputs Enables two-way communication between microcontroller and OLED for displaying data, menus, and status information

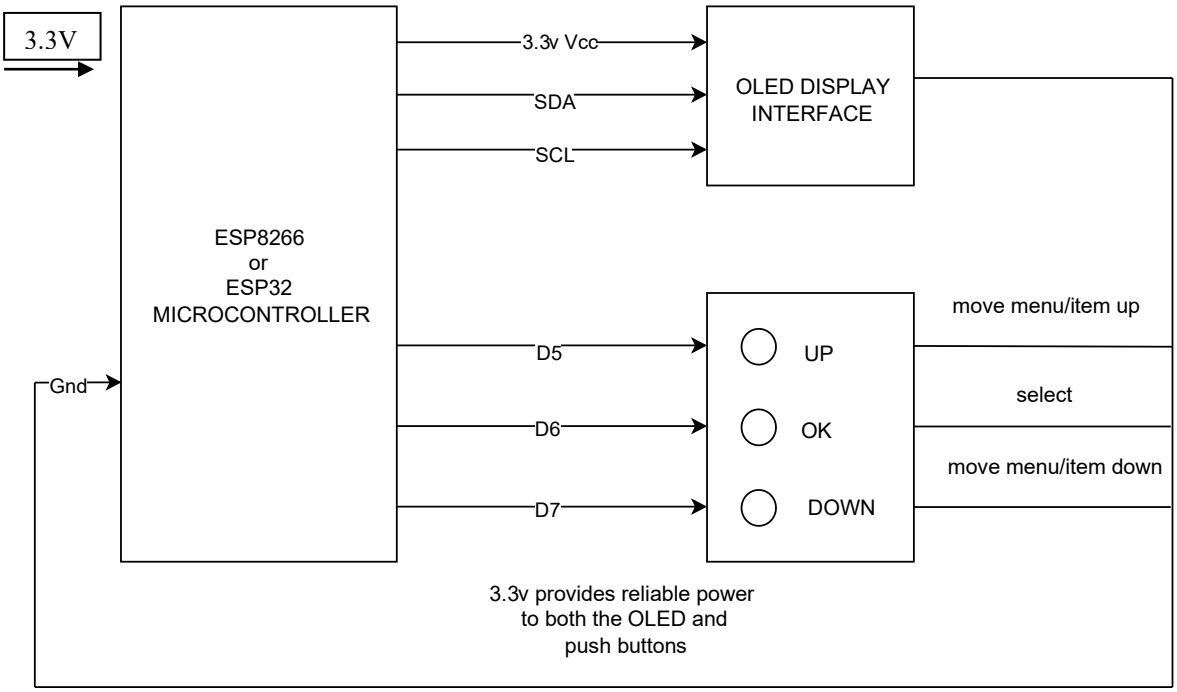

FIG 1. ARCHITECTURE DIAGRAM

III. IMPLEMENTATION

A. Hardware Components

The device utilizes an ESP8266 microcontroller (NodeMCU) as the main processing unit, an SSD1306 OLED display for visualization, and push buttons for user input. The system is powered via a USB connection or external battery, making it portable and suitable for field testing.

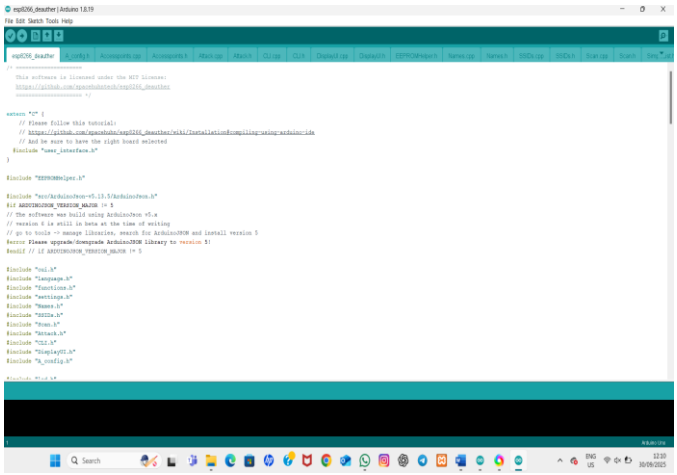

FIG 2. ARDUINO IDE

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121019

B. Software Development

Firmware is developed using the Arduino IDE with C++ programming language. Key libraries include the ESP8266WiFi library for network operations and the Adafruit_SSD1306 library for display control. The software implements packet crafting algorithms to generate valid deauthentication frames that comply with the 802.11 standard.

C. System Integration

All modules are integrated into a single firmware that manages the device's operation flow: initialization, network scanning, target selection, and attack execution. The system includes error handling mechanisms to ensure stable operation and prevent crashes during extended use.

IV. RELATED WORK

A. Commercial Penetration Testing Tools

Professional tools like Aircrack-ng suite and Kismet have long included deauthentication capabilities. While highly effective, these tools typically require Linux systems and technical expertise, making them less accessible for educational demonstrations and quick security assessments.

B. ESP8266-Based Security Projects

Previous projects have demonstrated the ESP8266's capability for packet injection and deauthentication attacks. However, many implementations lack user-friendly interfaces and require command-line operations or external computer control, limiting their standalone utility.

C. Educational Security Demonstrators

Academic institutions have developed various wireless security demonstrators, but these often focus on theoretical concepts rather than practical, hands-on tools. There remains a gap in providing portable, intuitive devices specifically designed for ethical hacking education.

D. Open-Source WiFi Testing Tools

Projects like WiFi-Pumpkin and various GitHub repositories offer deauthentication capabilities, but these typically require Raspberry Pi setups or complex software installations, reducing their portability and ease of use for quick demonstrations.

V. PROPOSED METHODOLOGY

A. Hardware Selection and Integration

ESP8266 NodeMCU for WiFi capabilities and processing powerSSD1306 OLED display for visual feedback Tactile push buttons for user interaction Portable power supply for field operation

B. Software Architecture

Modular firmware design separating scanning, attack, and UI functions Implementation of IEEE 802.11 frame crafting algorithms User interface state management for intuitive operation Error handling and input validation

C. System Development Phases

Prototype Development: Basic deauthentication functionality Interface Implementation: OLED display and button controls Feature Enhancement: Network scanning and target selection Testing and Validation: Performance evaluation and bug fixes

D. Ethical Considerations

Implementation of usage warnings and educational disclaimers Design focused on security awareness and education Clear documentation emphasizing legal and ethical use

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121019

VI. SYSTEM WORKFLOW

The operational workflow follows a systematic process:

System Initialization → Hardware components initialize and display startup screen

Network Scanning → ESP8266 scans for available WiFi networks and connected clients

Target Selection → User navigates through detected networks using push buttons

Attack Configuration → User selects attack parameters (duration, target type)

Deauthentication Execution → System sends crafted deauth frames to selected target

Status Monitoring → OLED display shows attack progress and statistics

Session Completion → System returns to scanning mode or powers down

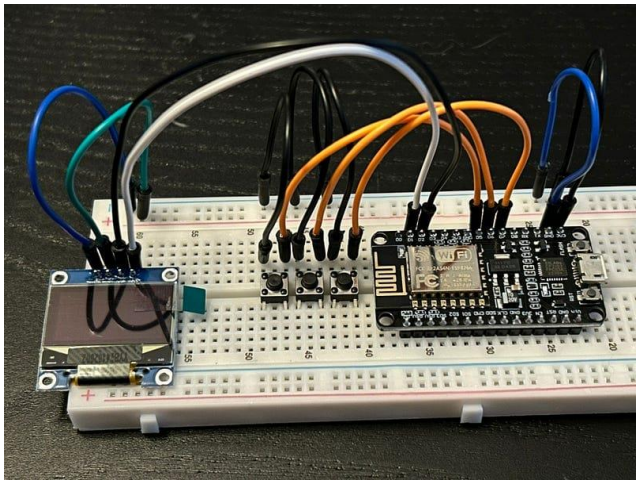

FIG 3. HARD WARE CONNECTION

VII. FUTURE WORK

A. Advanced Attack Modules
Implementation of beacon flood attacks for network disruption Addition of PMKID hash capture for WPA/WPA2 penetration testing Development of evil twin access point functionality

B. Enhanced User Experience
Integration of rotary encoder for smoother menu navigation Addition of audio feedback using buzzer or speaker Implementation of SD card logging for session records

C. Remote Control Capabilities
Web interface integration for wireless control Bluetooth connectivity for mobile app integration Development of automated scripting for complex test scenarios

D. Security Enhancements
Implementation of WPA3 security testing capabilities Addition of detection evasion techniques Development of defensive mechanism demonstrations

E. Educational Features
Integration of tutorial modes with step-by-step guidance Addition of security concept explanations and best practices Development of quiz and assessment functionalities

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121019

F. Hardware Improvements

Custom PCB design for compact form factor

Batter

VIII. CONCLUSION

This project successfully demonstrates the practical implementation of a WiFi deauthentication attack using the ESP8266 microcontroller, showcasing key concepts in wireless security and ethical hacking. Through modular design—including scanning, attack execution, and user interface modules—the system remains extensible, educational, and suitable for demonstration

purposes.Future improvements may include:

- Integration of additional attack vectors beyond deauthentication
- Enhanced logging capabilities for forensic analysis
- Remote control via web interface or mobile application
- Implementation of countermeasure detection algorithms
- Support for the latest WiFi standards and security protocols

XI. ACKNOWLEDGMENT

We thank the Department of IT and Kongunadu College of Engineering and Technology for infrastructural support. Special gratitude to our guide **Mr. VIKRAM P** for mentorship throughout the project.

REFERENCES

[1]. Ramafiarisona, H. M., & Rakotondramanana, R. S. (2024). WiFi Pentesting Roadmap for Classic-Future Attacks and Defenses. American Journal of Networks and Communications, 13(1), 44–63.

[2]. Surve, N., & Johnson, C. (2025). Security and Countermeasures against De-authentication Attacks. Journal of Emerging Technologies and Innovative Research (JETIR), 12(2).

[3]. Journal of Research and Analytical ReviewsKhandelwal, Y., Jossy, S., & Nair, A. C. (2024). Design and Implementation of Wi-Fi Deauthentication System Using NodeMCU ESP8266. International .

[4]. Vinjosh Reddy, S., Ramani, K. S., Rijutha, K., Mohammad Ali, S., & Pradeep Reddy, C. H. (2010). Wireless Hacking: A WiFi Hack by Cracking WEP. (Referenced in AJNC article)

[5]. tedsoftware. (2023). WiFiAttack: A Compact WiFi Deauthentication Tool. GitHub Repository

[6]. Alshamrani, A., & Alasmary, W. (2021). Wireless Network Security: Deauthentication Attacks and Countermeasures. International Journal of Computer Applications, 183(1), 25–30.

[7]. Khan, M. A., & Pathan, A. S. K. (2020). Securing Wi-Fi Networks Against Deauthentication Attacks Using 802.11w. Journal of Network and Computer Applications, 150, 102497.

[8]. Kumar, R., & Singh, P. (2022). Ethical Hacking Techniques for Wireless Networks. International Journal of Advanced Research in Computer Science, 13(2), 45–52

[9]. Gupta, S., & Sharma, V. (2023). IoT Security: Impact of WiFi Deauthentication Attacks on Smart Devices. Journal of Cybersecurity and Privacy, 3(1), 1–15.

[10]. Sharma, A., & Mehta, R. (2021). Wi-Fi Protected Access 3 (WPA3): A Comprehensive Security Framework. IEEE Access, 9, 123456–123470.

BIOGRAGHY

Mr. Vikram P is an Assistant Professor in the Department of Information Technology at Kongunadu College of Engineering and Technology, Tamil Nadu, India. His academic and research interests include Cybersecurity, Wireless Networks, Ethical Hacking, and Embedded Systems. He has guided several student projects related to network security and IoT-based ethical hacking tools, contributing to applied research and innovation in the field of information security education.

Mohamed Faize A is a pre final year B.Tech student in the Department of Information Technology at Kongunadu College of Engineering and Technology. His research interests include Network Security, Ethical Hacking, and Wireless Communication Systems. He has participated in various cybersecurity workshops and hackathons.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121019

Thiruvikram S is a pre final year B.Tech student in the Department of Information Technology at Kongunadu College of Engineering and Technology. His areas of interest include Cybersecurity, Embedded Systems, and IoT Security. He has worked on multiple projects related to network security and penetration testing.

Kabilan M is a pre final year B.Tech student in the Department of Information Technology at Kongunadu College of Engineering and Technology. His research focuses on Wireless Security, Microcontroller Programming, and Ethical Hacking Tools Development. He has expertise in ESP8266 programming and network protocol analysis.

