Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Slipper Zero+: Esp32-Based Wi-Fi Penetration and Defense Toolkit

Irfan R. S
Department of Computer Science and Engineering (Cyber Security)
Rajadhani Institute of Engineering and Technology
Trivandrum, Kerala, India

Aromal H
Department of Computer Science and Engineering (Cyber Security)
Rajadhani Institute of Engineering and Technology
Trivandrum, Kerala, India

Midhil V. P
Department of Computer Science and Engineering (Cyber Security)
Rajadhani Institute of Engineering and Technology
Trivandrum, Kerala, India

Biji Babu
Assistant Professor, Department of Computer Science and Engineering
Rajadhani Institute of Engineering and Technology
Trivandrum, Kerala, India

K. S Devanand
Department of Computer Science and Engineering (Cyber Security)
Rajadhani Institute of Engineering and Technology
Trivandrum, Kerala, India

Abstract **- Slipper Zero+ is a low-cost, portable Wi-Fi penetration and defence toolkit developed on the ESP32 microcontroller to demonstrate and analyze wireless security threats in real time. The system implements common penetration testing techniques such as deauthentication attacks and rogue access point simulation, highlighting vulnerabilities in widely used wireless networks. Unlike conventional tools that focus only on offensive operations, Slipper Zero+ integrates a lightweight intrusion detection mechanism capable of identifying abnormal patterns such as deauthentication floods and suspicious network behavior, providing real-time alerts to the user. Featuring a modular architecture and a user-friendly web-based dashboard, the system enables real-time monitoring, control, and visualization of wireless activities. It serves as both an educational platform for understanding Wi-Fi security concepts and a practical tool for evaluating network resilience. By combining offensive testing and defensive monitoring within a single embedded framework, Slipper Zero+ demonstrates the dual role of IoT-based hardware in cybersecurity analysis while promoting ethical, controlled, and hands-on experimentation.**

Keywords - Wi-Fi Security, ESP32, Deauthentication Attack, Intrusion Detection System, Rogue Access Point, Packet Sniffing, Embedded Security.

I. INTRODUCTION

Wireless communication has become an essential component of modern digital infrastructure, enabling seamless connectivity across devices, applications, and services. The widespread adoption of Wi-Fi networks in homes, enterprises, and IoT environments has significantly improved accessibility and convenience. However, this rapid growth has also introduced serious security challenges, making wireless networks a prime target for cyber-attacks [3].

Unlike wired networks, wireless communication operates over open radio frequencies, making it inherently vulnerable to attacks such as deauthentication, spoofing, rogue access points, and unauthorized access. Attackers can exploit these vulnerabilities to disrupt network availability, capture sensitive information, or gain unauthorized control over connected devices [2], [3].

Existing penetration testing tools such as Aircrack-ng, Wireshark, and Reaver provide comprehensive capabilities for analyzing wireless vulnerabilities. However, these tools require high-performance systems, external Wi-Fi adapters supporting monitor mode, and complex configurations, which limits their usability for beginners, students, and lightweight deployment scenarios. Furthermore, most traditional tools focus primarily on offensive security testing and lack integrated mechanisms for detecting attacks in real time [1], [5]. This creates a gap in practical cybersecurity education, where users can perform attacks but cannot simultaneously observe and analyze network behavior.

To address these limitations, this paper proposes Slipper Zero+, a portable ESP32-based system that integrates both penetration testing and intrusion detection capabilities. The system enables users to perform controlled wireless attacks while monitoring network traffic and detecting anomalies through a unified interface. By combining offensive and defensive features into a single embedded platform, the proposed system provides a comprehensive solution for wireless security analysis, aligning with recent research efforts in IoT-based security frameworks [5].

II. RELATED WORK

Recent studies have explored wireless network vulnerabilities, attack mechanisms, and IoT-based security solutions. The work in [1] presents an ESP32-based penetration testing tool capable of performing attacks such as deauthentication, PMKID capture, and rogue access point creation. It demonstrates that low-cost embedded devices can effectively execute complex Wi-Fi attacks, highlighting accessibility and emerging security risks in wireless networks. However, the study primarily focuses on offensive capabilities and does not incorporate real-time detection or mitigation

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

mechanisms, limiting its effectiveness for comprehensive security analysis.

The study in [2] focuses on detecting deauthentication denial-of-service attacks in IEEE 802.11 networks. It proposes a lightweight intrusion detection approach that monitors abnormal traffic patterns and identifies attack behavior with high accuracy, emphasizing the importance of real-time detection mechanisms in wireless security.

A comprehensive survey in [3] analyzes Man-in-the-Middle (MITM) attacks across various network environments. It categorizes attack techniques, discusses their impact on confidentiality and integrity, and reviews existing countermeasures, demonstrating that MITM attacks remain a persistent and evolving threat in modern communication systems.

The work in [5] examines IoT network security challenges and proposes an ESP8266-based penetration testing device along with a defense framework. It highlights key threats, risks, and vulnerabilities in IoT environments while emphasizing the need for integrated offensive and defensive approaches to improve network resilience.

Additionally, [4] represents general research contributions in the domain of network security and standardization, indicating ongoing efforts to address evolving threats and improve security frameworks.

Overall, these studies reveal that while significant progress has been made in understanding wireless attacks and developing penetration testing tools, there is still a lack of unified systems that combine both attack simulation and real-time intrusion detection. This gap motivates the development of integrated solutions such as the proposed system.

III. METHODOLOGY

The proposed system introduces a portable and embedded Wi-Fi security framework designed to perform both penetration testing and intrusion detection using an ESP32 microcontroller. The system operates as an independent wireless analysis unit capable of scanning, monitoring, attacking, and analyzing Wi-Fi networks in real time. The ESP32 serves as the core processing unit, enabling packet capture, packet injection, and communication with the control interface.

The system begins by initializing the Wi-Fi module and enabling promiscuous mode, allowing the capture of all wireless packets within range. These packets are processed to extract relevant information such as SSID, MAC address, channel, signal strength, and encryption type. The extracted data is used to build a structured representation of the surrounding wireless environment.Based on user input, the system operates in either detection mode or attack mode. In detection mode, the system continuously monitors network traffic and analyzes packet patterns to identify anomalies. In attack mode, the system generates and injects custom packets to simulate various wireless attacks such as deauthentication, beacon flooding, and rogue access point creation.

The system also includes a web-based dashboard that provides real-time interaction and visualization. The dashboard communicates with the ESP32 through a backend server, enabling users to control operations and monitor results efficiently.

A. Network Scanning Module

The network scanning module is responsible for identifying and analyzing all wireless networks within the communication range of the ESP32 device. The module performs active scanning by iterating through available Wi-Fi channels and capturing beacon frames transmitted by access points. These beacon frames contain essential information such as SSID, BSSID, channel, signal strength, and encryption type.

The module processes the captured data and organizes it into a structured format for display on the dashboard. Continuous scanning ensures that the system remains updated with changes in the wireless environment, including newly detected networks or changes in signal strength. This dynamic updating mechanism enhances situational awareness and enables users to make informed decisions during analysis and attack execution.

B. Packet Sniffing and Intrusion Detection Module

The packet sniffing module operates in promiscuous mode, capturing all wireless frames within range, including management, control, and data packets. These packets are processed to extract key parameters such as source and destination MAC addresses, frame types, sequence numbers, and signal strength. By continuously monitoring this information, the system identifies traffic patterns and behavioral trends, enabling the detection of unusual or suspicious network activities in real time.

The intrusion detection mechanism employs threshold-based analysis to identify anomalies such as a sudden surge in deauthentication frames, repeated connection attempts, or irregular packet sequences. It can also correlate multiple indicators to improve detection accuracy and minimize false positives. Upon detecting suspicious activity, the system generates real-time alerts through a web-based dashboard and hardware indicators like LEDs or buzzers, while maintaining basic logs for later analysis and investigation.

C. Attack Simulation Module

The attack simulation module enables controlled execution of various wireless attacks for testing and educational purposes. The module generates custom Wi-Fi frames and injects them into the network using the ESP32's packet injection capability. Supported attacks include deauthentication, beacon flooding, and rogue access point simulation.

The module allows users to select target networks and configure attack parameters through the dashboard. This flexibility enables controlled experimentation and analysis of network vulnerabilities. The system ensures that attack execution is managed efficiently, maintaining stability and preventing unintended disruptions beyond the test environment.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

D. *Control and Dashboard Module*

The control module consists of a web-based dashboard that provides a centralized interface for system interaction and monitoring. The dashboard is implemented using Flask for backend communication and HTML, CSS, and JavaScript for frontend visualization.

The interface allows users to perform various operations such as initiating scans, selecting targets, executing attacks, and monitoring alerts. Real-time updates are displayed through dynamic components, enabling users to observe network activity and system performance continuously.

IV. SYSTEM DESIGN AND ARCHITECTURE

A. *Design Overview*

The Slipper Zero+ device is a compact, portable system built around the ESP32 microcontroller, integrating both penetration testing and intrusion detection functionalities within a single platform. The design follows a modular architecture, enabling easy assembly, maintenance, and future scalability. The ESP32 module acts as the central processing unit, handling wireless packet sniffing, attack execution, and real-time traffic analysis. It supports multiple operating modes, allowing users to seamlessly switch between monitoring and attack functionalities based on requirements. The system operates using a dedicated power input and is interconnected through a custom wire harness that efficiently distributes power and GPIO signals to all peripheral components. A toggle switch is included to provide simple and reliable control over device operation, enhancing usability during field testing and demonstrations.

For user interaction and feedback, the system incorporates an LED module and a buzzer to indicate various operational states such as scanning, attack mode, and anomaly detection. These hardware indicators provide immediate real-time alerts, complementing the web-based monitoring interface that enables users to visualize network activity, configure parameters, and control system functions remotely. Additionally, the system maintains basic logs of detected events, allowing users to review past activities and analyze attack patterns. All components are securely enclosed within a 3D-printed casing consisting of a base and a removable top cover, fastened using screws for structural stability. The enclosure is designed to ensure durability, portability, and proper component alignment while allowing adequate ventilation for heat dissipation. Overall, the design emphasizes efficiency, flexibility, and seamless integration, making it suitable for both practical wireless security analysis and educational applications.

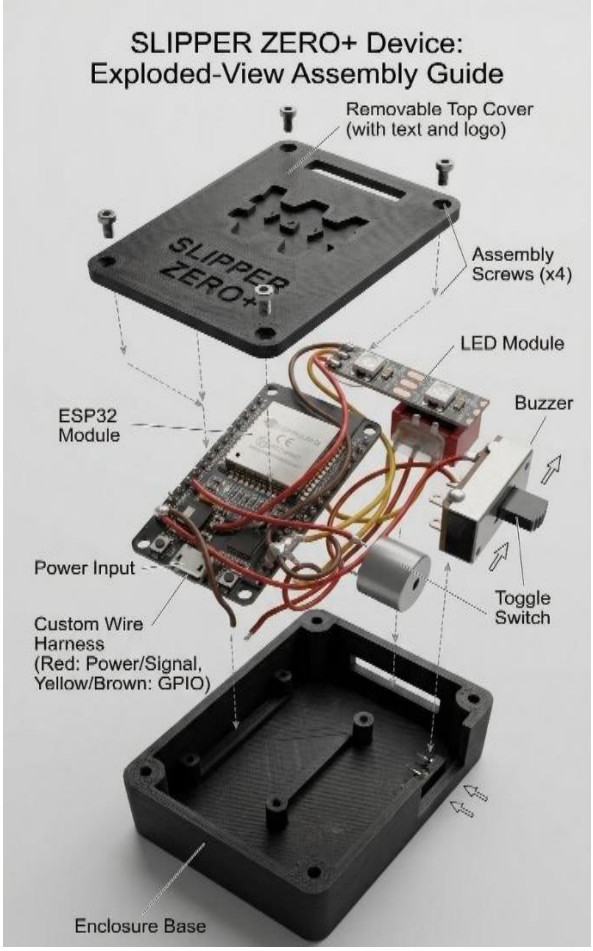

Fig. 1. Structural Design and Component Integration of Slipper Zero+

B. *System Architecture*

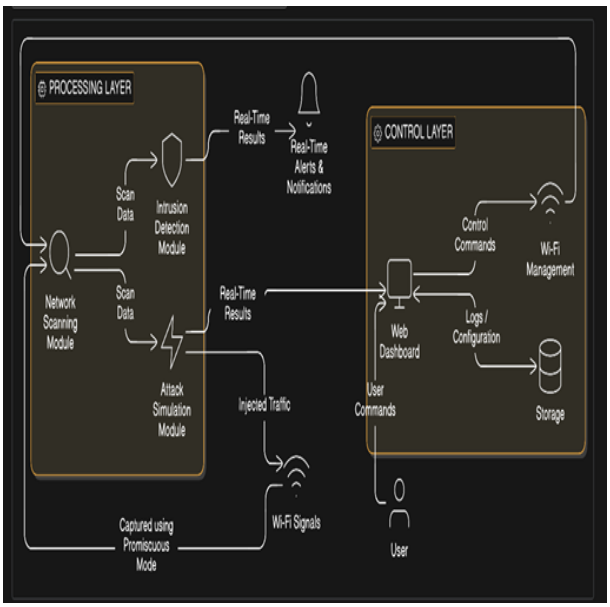

Fig. 2. System Architecture of Slipper Zero+ Device

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The architecture of the proposed system is composed of interconnected modules that operate in a coordinated manner to ensure efficient wireless security analysis. The system is divided into processing and control layers.

The processing layer includes modules for network scanning, packet sniffing, intrusion detection, and attack simulation. The ESP32 captures wireless packets, processes data, and executes attack operations. The intrusion detection module analyzes packet behavior to identify anomalies.

The control layer consists of the web dashboard, which acts as the interface between the user and the system. It sends control commands to the ESP32 and receives real-time updates. The communication between layers is achieved through serial and WebSocket protocols.The system also integrates hardware alert components such as LEDs and buzzers to provide immediate feedback during operation.

V. SYSTEM IMPLEMENTATION

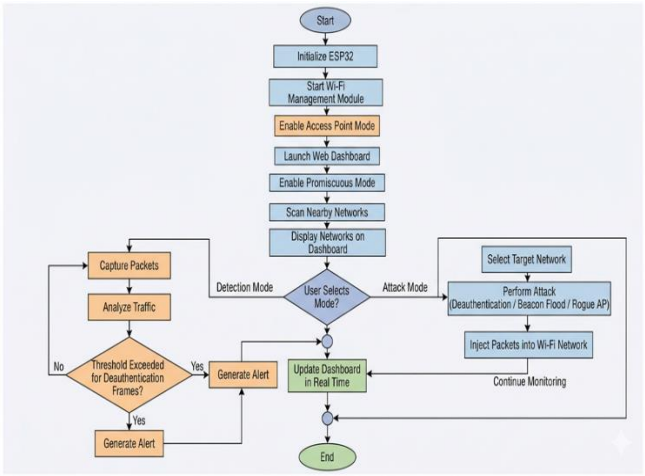

Fig. 3. Implementation Flow of Slipper Zero+ Device

The implementation of the Slipper Zero+ system is carried out on the ESP32 microcontroller, integrating both wireless attack simulation and intrusion detection functionalities. The system begins by initializing the ESP32 and activating the Wi-Fi management module, followed by enabling access point mode to host a web-based dashboard. The dashboard allows users to interact with the device, configure parameters, and monitor real-time wireless activity. The ESP32 is then set to promiscuous mode, enabling it to capture all nearby Wi-Fi packets and scan available networks, which are displayed to the user through the interface.

Based on user selection, the system operates in either detection mode or attack mode. In detection mode, captured packets are analyzed continuously to identify anomalies such as excessive deauthentication frames using a threshold-based approach. When abnormal behavior is detected, alerts are generated and displayed in real time on

the dashboard. In attack mode, the user selects a target network and initiates actions such as deauthentication or beacon flooding, where packets are injected into the network for controlled testing. The system maintains continuous monitoring during both modes, updating the dashboard dynamically and ensuring seamless interaction between analysis, alert generation, and user control.

VI. RESULT

Fig. 4. Prototype of Slipper Zero+ Device

The proposed system was evaluated in a controlled wireless environment to assess its performance and reliability, focusing on network scanning accuracy, attack execution capability, and intrusion detection effectiveness. The network scanning module successfully detected multiple access points and provided detailed real-time information while maintaining stable performance during continuous updates. The attack module effectively executed deauthentication and beacon flooding attacks, demonstrating reliable packet injection and allowing dynamic user control without performance degradation. The intrusion detection module accurately identified abnormal traffic patterns, including high-frequency deauthentication frames and unusual packet behavior, generating real-time alerts with clear visualization on the dashboard. Additionally, the rogue access point module successfully captured credentials in a controlled setup, validating the system's ability to simulate real-world attack scenarios. Overall, the system demonstrated consistent performance, accurate detection, and efficient user interaction.

VII. FUTURE ENHANCEMENTS

The proposed system can be further enhanced by integrating advanced technologies and extending its capabilities. One potential improvement is the incorporation of AI/ML-based intrusion detection techniques to identify complex and evolving

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Wi-Fi attacks through intelligent analysis of traffic patterns and anomalies. Additionally, support for WPA3 security can be implemented to enable testing and evaluation of modern wireless networks, ensuring compatibility with emerging security standards.

Another significant enhancement is the integration of cloud-based monitoring, allowing centralized logging, real-time analysis, and remote alert management through web-based platforms. These improvements would increase the system's scalability, accuracy, and adaptability, making it more effective for real-world cybersecurity applications and research purposes.

VIII. CONCLUSION

This paper presents a portable and integrated Wi-Fi penetration testing and intrusion detection system using the ESP32 platform. The proposed system combines packet sniffing, attack simulation, and anomaly detection into a unified framework, addressing the limitations of traditional tools.

By enabling real-time monitoring and controlled attack execution, the system provides a comprehensive solution for wireless security analysis. The use of a web-based dashboard enhances usability and accessibility, making the system suitable for both beginners and professionals.

The implementation demonstrates that advanced wireless security functionalities can be achieved using low-cost embedded hardware. The system serves as an effective platform for cybersecurity education, research, and practical network auditing.

REFERENCES

[1] https://www.researchgate.net/publication/387481539_Slipper_Zero_Exploring_WiFi_Security_Vulnerabilities_and_Attack_Implementations_on_ESP32_Microcontrollers

[2] https://www.researchgate.net/publication/269331936_Detection_of_Deauthentication_Denial_of_Service_attack_in_80211_networks?utm_source=chatgpt.com

[3] https://orbit.dtu.dk/en/publications/a-survey-of-man-in-the-middle-attacks/?utm_source=chatgpt.com

[4] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[5] https://www.researchgate.net/publication/372974082_Analysis_on_IoT_Networks_Security_Threats_Risks_ESP8266_based_Penetration_Testing_Device_and_Defense_Framework_for_IoT_Infrastructure