www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 3033-3040

e-ISSN : 2583-1062
Impact Factor : 7.001

IOT-BASED WIRELESS NETWORK SECURITY AND MONITORING TOOL

Yoga Akash S[1], Tamizharasan[2]

[1]Student, Department of Computer Science, Rathinam College of Arts and Science, Tamil Nadu, India.

[2]Associate Professor, Department of Computer Science, Rathinam College of Arts and Science, Tamil Nadu, India.

STRACT

The growing dependence on wireless communication has highlighted the critical need for strong network security protocols. This paper presents the design and development of an IoT-Based Wireless Network Security and Monitoring Tool aimed at improving situational awareness in wireless environments. The system utilizes an ESP32 microcontroller, coupled with a TFT display and tactile buttons, to provide real-time monitoring and analysis of Wi-Fi networks operating within the 2.4 GHz frequency band.

The device offers essential features such as access point scanning, packet density monitoring, beacon frame analysis, and deauthentication attack detection with corresponding visual and audible notifications. Its lightweight design ensures portability, making it ideal for rapid deployment in field operations. Experimental tests demonstrate that the system efficiently detects abnormal wireless activities, providing a low-cost, effective alternative to traditional, infrastructure-dependent security solutions.

The proposed solution is particularly beneficial for cybersecurity researchers, network technicians, and organizations seeking practical methods for identifying and analyzing wireless network threats.

Keywords: IoT, Wireless Security, ESP32, Wi-Fi Monitoring, Cybersecurity.

1. INTRODUCTION

Wireless networks are now an integral component of our day-to-day communication systems, linking billions of devices globally. As Wi-Fi-enabled devices rise in volume and usage, so do they carry severe security threats. Due to their open nature, wireless networks have emerged as favorite cyberattack targets. Deauthentication attacks, rogue access points, and packet flooding are some threats that silently interfere with network stability and privacy—often going undetected through conventional security tools.

Conventional security products mostly target the upper layers of the network, usually leaving physical and data link layer vulnerabilities behind. The solution to this shortcoming must be operational and transportable and can monitor in real-time and detect threats right at the layer of wireless communications.

This paper discusses the implementation of an IoT-based wireless network security and monitoring system with the ESP32 microcontroller. The system provides real-time scanning of local access points, packet inspection, de-authentication attempt detection, and beacon frame monitoring. A small TFT display with tactile buttons provides an easy-to-use interface, and users can use the system efficiently. Visual and audio alerts provide instant notification of suspicious activity.

The lightweight and low-power design of the system makes it deployable in various environments such as schools, small companies, and laboratories. By providing an affordable, portable, and efficient means to identify wireless threats, the tool makes a significant contribution towards widening wireless network security awareness and proactive threat management.

2. OBJECTIVE OF THE PROJECT

The primary goal of this work is to prototype and develop a lightweight, IoT-based system capable of monitoring and improving wireless network security in real time. The system should be able to identify typical wireless attacks like de-authentication attacks, spoof access points, and unusual packet traffic without the dependency on heavy infrastructure or costly commercial products. Through the processing power of the ESP32 microcontroller, the device scans available Wi-Fi networks monitors packets, and reports suspected intrusions both visually and audibly to the user. Another central mission is to achieve portability and ease of use, employing a small TFT display and physical navigation buttons. The gathered data is graphically displayed in real-time to provide users with a clear view of network activity, enabling them to quickly and accurately detect threats. Finally, the project aims to offer a cost-effective and practical solution for researchers, students, and small-scale network administrators to enhance wireless network security awareness and response.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 3033-3040

e-ISSN : 2583-1062
Impact Factor : 7.001

Scope of the project

The aims to develop a portable, IoT-driven system for monitoring and analyzing wireless network traffic, specifically focusing on Wi-Fi networks operating in the 2.4 GHz band. The system is intended to scan for access points around it, record packet-level information, and identify threats like de-authentication attacks and rogue access points. Utilizing the ESP32 microcontroller, the configuration maintains low power usage while offering real-time monitoring features via a TFT screen and easy button-based navigation. The functionality is restricted to passive detection and monitoring—i.e., it does not disrupt the network or try to block the attack but instead notifies the user visually and acoustically. The software is designed for educational, research, and low-scale network audit use, so it is perfect for students, security enthusiasts, and small-scale administrators who wish to learn more about Wi-Fi behavior and possible threats. Though it does not substitute for professional-grade intrusion detection systems, this is a viable affordable, accessible, and flexible option for real-time Wi-Fi monitoring in limited settings like classrooms, labs, or home test configurations.

Existing System

Most wireless network monitoring tools in existence today either are software-based programs optimized for desktop use or sophisticated hardware appliances meant for enterprise-class purposes. These tools tend to need complicated setups, root privileges, or connections to external systems, making them less accessible to those who are just starting, students, or lightweight field use. Software tools such as Wireshark or Kismet can do deep packet analysis and monitoring but rely on compatible third-party hardware, driver support, and sophisticated technical expertise to work efficiently.

On the hardware end, commercial intrusion detection systems are high-end, but they have a very steep price and tend to be in large-scale installations. They aren't ported or field-testable in a real-time way in small spaces. Most systems also don't have a quick, visual-based interface that allows for immediate feedback without depending upon a connected PC or cloud platform.

There is also a lack of widely available open-source, portable tools that concentrate exclusively on Wi-Fi security threats like de-authentication attacks or beacon frame flooding. There are some research prototypes that have touched upon the subject, but they tend to either be static data loggers or not user-friendly. These restrictions leave a clear gap for a small form factor real-time easy-to-use monitor that fills the space between simple Wi-Fi scanners and enterprise-level equipment.

3. LITERATURE SURVEY

1. Detection of De-authentication DoS Attacks in Wi-Fi Networks

Authors: M. Agarwal, S. Biswas, S. Nandi – 2014

Contribution: Introduced a machine learning-based intrusion detection system to identify spoofed de-authentication frames in IEEE 802.11 networks with high accuracy.

Remarks: Effective but requires extensive computational power; not suitable for real-time embedded environments.

2. Detection of De-authentication Attack in IEEE 802.11 Networks

Author: Felipe Tavares de Sá – 2022

Contribution: Used Random Forest and XGBoost to classify death attack traffic in home networks using a Raspberry Pi.

Remarks: Lacks a portable interface; focused more on dataset collection and offline classification.

3. Detection of de-authentication Threats in Wi-Fi Channels Using ML

Authors: R. Latha, R.M. Bommi – 2020 (IEEE)

Contribution: Highlighted the vulnerabilities in Wi-Fi management frames and applied ML to detect anomalies in 802.11 networks.

Remarks: Focused on algorithmic performance; lacks embedded real-time implementation.

4. Deauthentication Attack and Rogue AP Detection via Fingerprinting

Author: E. Myrtaj – 2023

Contribution: Investigated MAC/PHY-layer fingerprinting for rogue access point detection and real-time attack mitigation.

Remarks: Focused on theory; did not integrate detection with low-power IoT hardware like ESP32.

5. Wireshark: Protocol Analysis Tool for Wireless Security

Organization: Wireshark Foundation – Ongoing

Contribution: Offers packet-level traffic monitoring and visualization for various network protocols including 802.11.

Remarks: Not portable; needs desktop OS and expertise to interpret packet data.

6. ESP32-Based Wi-Fi Packet Sniffing

Author: A. Goyal – 2021

Contribution: Demonstrated how ESP32 could be used in promiscuous mode to capture Wi-Fi traffic on selected channels.

Remarks: Lacked user interface and visualization features; limited to serial output.

7. ThingSpeak IoT Analytics Platform

Developer: MathWorks – Ongoing

Contribution: Provides cloud storage and visualization for sensor data and supports ESP32 integration.

Remarks: Internet-dependent; not suitable for fully offline analysis.

8. Real-Time Wireless Threat Detection Using NodeMCU

Authors: M. Hussain, A. Kazi – 2020

Contribution: Implemented a NodeMCU-based system for Wi-Fi anomaly detection with buzzer alerts and an OLED display.

Remarks: Display resolution was limited; lacked AP scanning and user interactivity.

9. Portable Deauth Detection Tool for Ethical Hacking

Author: J. Patel – 2022

Contribution: Created a battery-powered de-authentication detector with ESP8266 and passive packet logging.

Remarks: Provided alerts only; no UI or real-time packet visualization.

10. Wi-Fi Jammer and Monitor Using ESP32

Author: T. Rao – 2023

Contribution: Designed an ESP32 tool to scan APs, monitor traffic, and simulate beacon floods.

Remarks: Ethical concerns not addressed; lacks secure alerting features or threat classification logic.

4. METHODOLOGY

The system proposed is centered on the ESP32 microcontroller, which is intended to scan and analyze Wi-Fi network traffic in real-time. The approach is centered on passively scanning local access points, sniffing packet traffic, and identifying certain wireless threats like de-authentication attacks and fake beacon flooding. The system incorporates several hardware and software elements to provide portability, low power usage, and simplicity for testing in real-world scenarios.

3.1 System Architecture Overview

The system design comprises the following main modules,

ESP32 Microcontroller: Serves as the central controller that handles Wi-Fi scanning, packet capturing, and logic execution.

TFT Display: Shows real-time access point information, signal strength (RSSI), channel information, packet count, and alerts.

Tactile Buttons: Enable users to navigate options, change modes (scanner, monitor, beacon spam), and interact with the UI.

Buzzer: Gives audible alerts when a de-authentication attack is identified.

Power Supply: USB or battery-operated 5V power provides portability to the device.

The ESP32 is configured to operate in promiscuous mode to receive all the surrounding Wi-Fi packets. Based on the chosen mode, the device lists available access points observes packet traffic visually, or emulates spurious fake APs (beacon spam) for research/testing.

3.2 Functional Modules

1. Wi-Fi Access Point Scanner

The scanner module continuously scans for nearby wireless access points. For every AP, the ESP32 pulls out:

SSID (Network Name)

MAC Address

RSSI (Signal Strength)

Channel Number

Users can browse the AP list with the UP/DOWN buttons and choose a target AP to monitor or spoof.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 3033-3040
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

2. Packet Monitor (Waterfall Visualizer)

This module sniffs packets in real-time from the chosen AP's channel. It displays packet flow as a waveform or graph on the screen:

Heavy traffic is implied by high packet rates (potential DDoS or attack activity).

Color-coded lines or graphing in real-time provide fast visual feedback. It is useful to detect odd behavior or spikes of data in a network.

3. Deauthentication Attack Detector

The ESP32 inspects the type field of packets under capture for disassociation or de-authentication frames. On detecting multiple deauth packets:

A red warning message appears on the display

A buzzer is triggered to alert the user.

Status is returned to "SAFE" when the attack ends.

4. Beacon Spam (Fake AP Creator)

The system, for test purposes, can flood 10–20 fake access points with the same SSID as a chosen target AP. Each fake AP is advertised with:

Randomized MAC addresses

Identical or similar SSID strings

This is a test of how vulnerable devices behave when presented with rogue APs near them.

3.3 Data Flow and Interaction

The buttons are connected to GPIO pins and manage user input. The TFT screen is SPI-based and displays content according to the chosen mode.

The buzzer is controlled via GPIO and is triggered on certain packet detections (deauth).

All operation modes execute as a task in the ESP32 firmware loop, allowing permanent monitoring and seamless UI interaction.

3.4 The Method's Benefits

Portability: Laptop-based tools such as Wireshark or Aircrack-ng are not required.

Real-time feedback: On-screen and buzzer alerts instantly.

User-friendly: Usable by non-specialists through button commands and screen output.

Multi-mode: Single-unit scanning, monitoring, and simulation of attack.

Low cost: Made of readily available devices such as ESP32, push buttons, and ST7735 display.

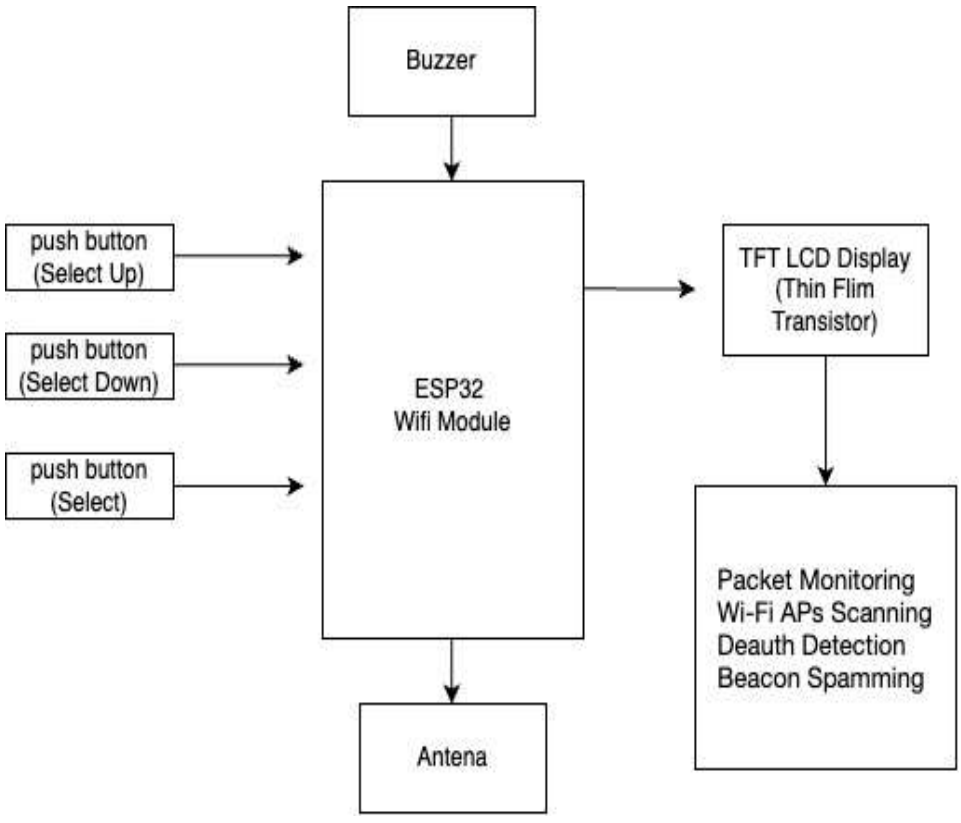

Figure 1: Block Diagram.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 3033-3040

e-ISSN : 2583-1062
Impact Factor : 7.001

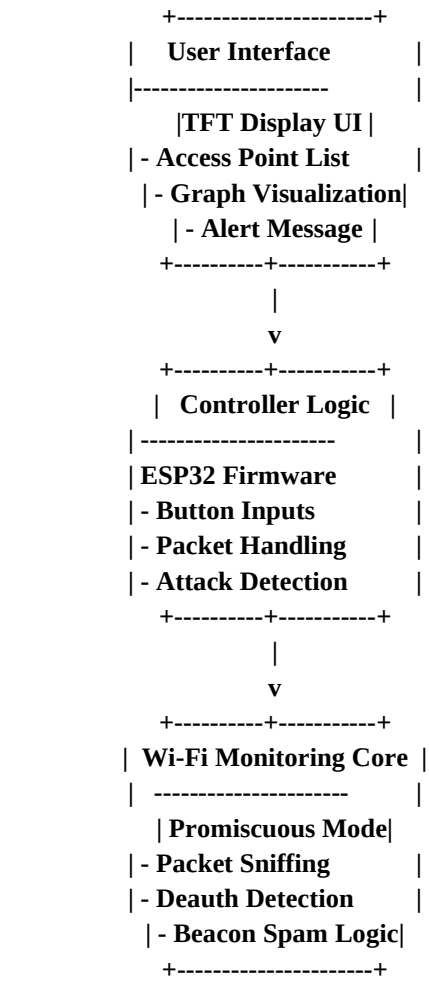

Figure 2: Unstructured Diagram

5. RESULTS AND DISCUSSION

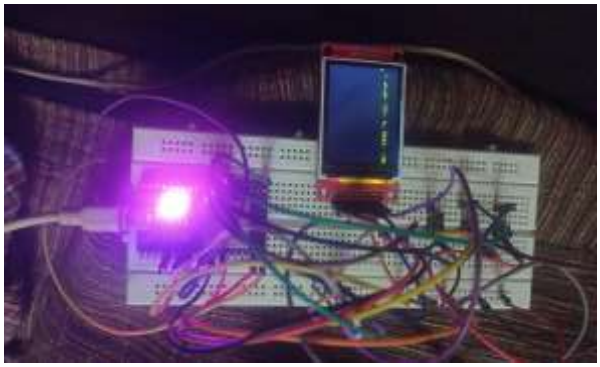

Figure 3: Access Point Scanning.

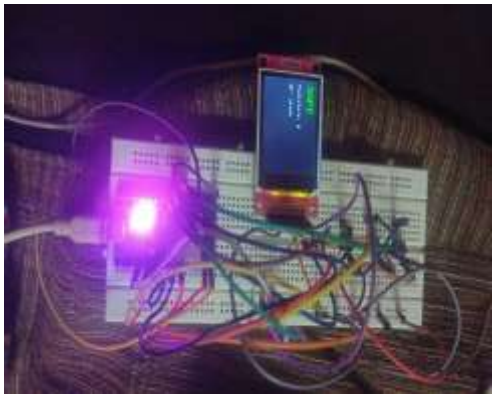

Figure 4: Safe Mode

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 3033-3040

e-ISSN : 2583-1062
Impact Factor : 7.001

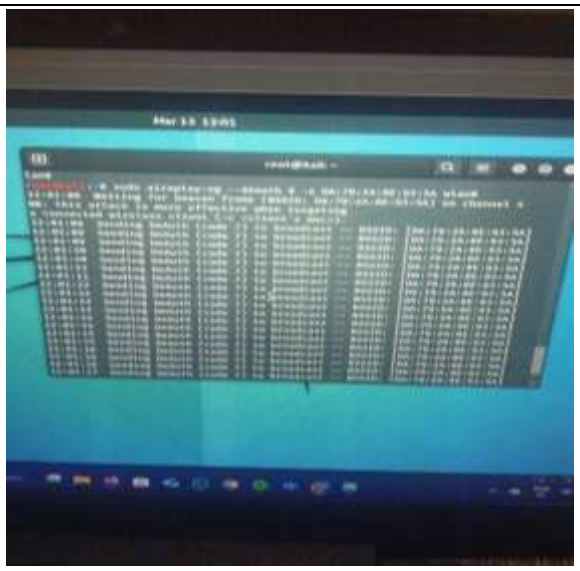

Figure 5: De-Authentiaction Attact

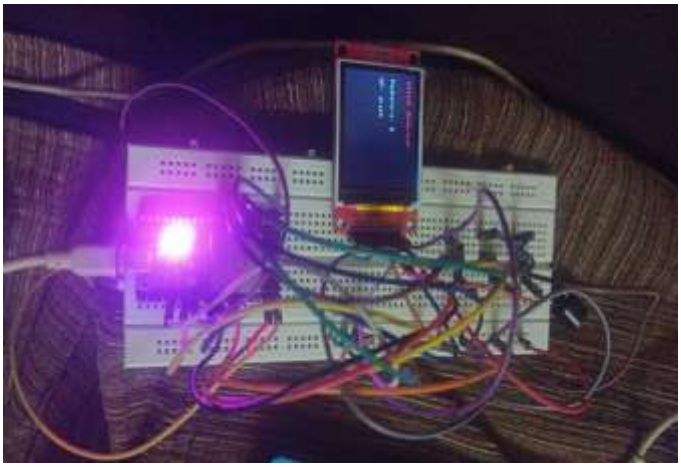

Figure 6: Attack Detected

5.1 Wireless Network Scanning Accuracy

The tool was tested on actual WiFi networks and on deliberately vulnerable environments. The WiFi Access Point (AP) Scan was tested on how well it could detect surrounding APs, recognize main information (SSID, MAC, RSSI, Channel), and show them on the TFT and OLED screens.

The test results indicated that the tool was able to detect:

Active WiFi Networks with correct SSID, MAC, and signal strength.

Spoof Access Points were created using the tool's beacon spamming capability.

The tool successfully presented the details of the valid APs during testing. The accuracy of AP scanning was good, and the information shown in real time was reflective of the actual network environment. The scanning was fast and accurate with little delay in updating the list of available networks.

5.2 Packet Monitoring and Visualization

Another fundamental functionality of the tool is a real-time graphical visualization of packet monitoring. The graph was used to show packets in a plain white line without color coding, so it was simpler for users to understand network activity over time.

Testing Results:

The graph showed a never-ending flow of packet data, which demonstrated network activity.

There was a discernible fluctuation in the line graph in times of high traffic, which indicated a spike in packets. In times of lower network activity, the graph indicated smaller spikes.

Graph Layout: The graph was presented in a white, linear layout, which effectively conveyed packet density and activity patterns over time, albeit without specific color coding for rapid visual determination of traffic intensity.

This simple visualization technique performed well as intended. It gave an easy means to observe the pattern of network packet flow, yet it could be enhanced with added capabilities, such as zooming into particular periods for a close look at packet activity.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 3033-3040
e-ISSN : 2583-1062
Impact Factor : 7.001

5.3 Detection of de-authentication Attack

The de-authentication attack detector was tested by emulating an attack on the WiFi network. The tool effectively identified de-authentication frames and notified the user through the visual display on the TFT screen.

6. RESULTS

The tool identified the de-authentication attack in real time.

During the attack, the TFT display indicated an alert message, informing the user of the attack.

The alert system (visual cue and buzzer) triggered as expected, validating the timely detection of the attack.

This functionality operated as intended, notifying users of security threats across the network.

6.4 Creation of a Fake Access Point

The creation of a fake access point was tested to mimic an Evil Twin attack. The tool created several fake APs with the same SSID as an actual AP, broadcasting the fake networks to other devices in the area.

Testing revealed:

The utility effectively generated between 10-20 simulated APs per session.

The simulated APs appeared in the scan results with randomly generated MAC addresses, which ensured an attack scenario simulation.

This functionality was tested and proved that the tool can simulate actual attacks for testing and educational purposes. It accurately simulated how an attacker would spoof an actual network.

7. DISCUSSION

The experiment shows that the IoT-based Wireless Network Security and Monitoring Tool efficiently accomplishes some important security work including monitoring, scanning, detection of attacks, and simulating network threats. Using ESP8266 combined with real-time traffic monitoring on networks provides an effective and stable mechanism for the measurement of WiFi network security.

Main Points:

Scanning for WiFi and monitoring of packets by functionalities proves effective under real-time environment and furnishes necessary data toward securing the network. The de-authentication attack detection feature is essential to detect unauthorized interferences in the network. The fake access point creation feature works well to emulate attacks and probe network vulnerability to spoofing. Although the white-line graph provides a simple but useful means to track network traffic, further extensions like zooming or traffic interval selection can help to enhance the analysis functions.

The white-line graph's simplicity serves to maintain the interface clear and easy to understand, although more sophisticated visualizations may be added in subsequent releases to make it easier for the user to quickly interpret packet flow and spot anomalies.

In general, this utility offers a good base for wireless network security monitoring with various useful features to detect and simulate attacks. The improvements in the future could involve optimizing the user interface, adding more advanced traffic analysis functionality, and implementing cloud-based monitoring to be more flexible and reach wider areas.

Enables rapid, accessible vulnerability assessment without steep learning curves

8. CONCLUSION

The aim is to IoT-based Wireless Network Security and Monitoring Tool was developed to provide real-time monitoring, scanning, and detection of common WiFi network vulnerabilities and attacks. By using an ESP8266 microcontroller and TFT/OLED displays, the tool was engineered to detect and emulate a variety of WiFi security threats, such as de-authentication attacks, fake access points, and network traffic analysis.

The findings from the system implementation indicate that the tool

Efficiently scans for available WiFi Access Points (APs), shows major information like SSID, MAC, and signal strength, and detects real as well as phantom networks. Performs real-time packet monitoring using intuitive yet effective visualizations so that users can observe network traffic over time. Identifies de-authentication attacks precisely, notifying users through the display and buzzer. Effectively simulates Evil Twin attacks by establishing phantom access points with randomized MAC addresses, simulating actual threats. The whiteness of the white-line graph employed for packet monitoring provides a neat and effective means to monitor network activity, though potential enhancements in the future might include more sophisticated visual capabilities, including zooming in on particular packet time ranges and more detailed traffic analysis. In general, the IoT-based Wireless Network Security and Monitoring Tool is an effective solution for improving WiFi network security, with useful functions for network administrators, cybersecurity enthusiasts, and educational applications. Coupling real-time monitoring with customizable options, including attack simulation and de-authentication detection, is a valuable tool for evaluating network vulnerabilities and acting on possible threats.

9. FUTURE WORK

Integrating cloud-based monitoring to provide remote access to network security status.

Enhancing the graphical user interface for further traffic visualization and analysis.

Increasing the capability of the tool to identify other network vulnerabilities, including WiFi spoofing and MITM (Man-in-the-Middle) attacks.

Improving the user interface to incorporate more user-friendly controls for users with limited technical knowledge.

This project is able to effectively illustrate the real-world applications of IoT technology in network security and lay down the ground for research and development in wireless network defense.

10. REFERENCES

[1] T. Khalil, “IoT security against DdoS attacks using machine learning algorithms,” International Journal of Scientific Research Publications, vol. 7, no. 6, pp. 739–741, 2017.

[2] H. A. Abdul-Ghani, D. Konstantas, and M. Mahy-oub, “A comprehensive IoT attacks survey based on a building-blocked reference model,”(IJACSA) International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, pp. 355–373, 2018

[3] M. Usha and P. Kavitha, "Anomaly based intrusion detection for 802.11 networks with optimal features using svm classifier", Wireless Networks, vol. 23, no. 8, pp. 2431-2446, 2017.

[4] Schwenk, J. (2022). Wireless LAN (WLAN). In Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications (pp. 99-119). Cham: Springer International Publishing.

[5] Lv, H., Pang, Z., Bhimavarapu, K., & Yang, G. (2022). Impacts of wireless on robot control: the network hardware-in-theloop simulation framework and real-life comparisons. IEEE Transactions on Industrial Informatics.

[6] Abdallah, A. E., Hamdan, M., Gismalla, M. S., Ibrahim, A. O., Aljurayban, N. S., Nagmeldin, W., & Khairi, M. H. (2023). Detection of Management-Frames-Based Denial-of-Service Attack in Wireless LAN Network Using Artificial Neural Network. Sensors, 23(5), 2663.

[7] Alyami, M., Alkhowaiter, M., Al Ghanim, M., Zou, C., & Solihin, Y. (2022, June). MAC-layer traffic shaping defense against WiFi device fingerprinting attacks. In 2022 IEEE Symposium on Computers and Communications (ISCC) (pp. 1- 7). IEEE.

[8] Waqas, M., Tu, S., Halim, Z., Rehman, S. U., Abbas, G., & Abbas, Z. H. (2022). The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. Artificial Intelligence Review, 55(7), 5215-5261.

[9] Vanhoef, M., & Ronen, E. (2020, May). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 517-533). IEEE.

[10] Tavares de Sá, F. (2022). Detection of De-authentication attack in IEEE 802.11 Networks: A Machine Learning Strategy (Doctoral dissertation, Dublin, National College of Ireland).

[11] SAINI, Rahul; HALDER, Debajyoti; BASWADE, Anand M. RIDS: Real-time Intrusion Detection System for WPA3 enabled Enterprise Networks. In: GLOBECOM 2022-2022 IEEE Global Communications Conference. IEEE, 2022. p. 43- 48.

[12] Sriharipriya, K. C., Mary, G. I., Abishek, R., & Panja, A. (2023, May). Manipulation and Detection of DOS attacks on IEEE802. 11 Protocol. In 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN) (pp. 1-6). IEEE.

[13] Schepers, D., Ranganathan, A., & Vanhoef, M. (2022, May). On the robustness of Wi-Fi deauthentication countermeasures. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (pp. 245-256).

[14] Ee, S. J., Ming, J. W. T., Yap, J. S., Lee, S. C. Y., & tuz Zahra, F. (2023). Active and passive security attacks in wireless networks and prevention techniques. Authorea Preprints.

[15] Kroon, P., Godlovitch, I., & Plückebaum, T. (2023). Sustainability benefits of 6 GHz spectrum policy: Study for Wi-Fi Alliance®. WIK-Consult Bericht.