Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Detect wi-fi De-Authentication Attacks Using Esp8266

Lakshmi Saranya, Reddyvari Venkateswara Reddy, A Basanth Reddy,
Bolloju Sai Dinesh, Mohammad Muneeruddin
Associate Professor, Department of CSE (Cybersecurity), CMR College of Engineering & Technology, Hyderabad, Telangana, India.
Associate Professor, Department of CSE (Cybersecurity), CMR College of Engineering & Technology, Hyderabad, Telangana, India.
Students, Department of CSE (Cybersecurity), CMR College of Engineering & Technology, Hyderabad, Telangana, India.

***Abstract*—In network security, the utilization of an ESP8266 microcontroller unit (MCU) from Espressif Systems emerges as a vigilant guardian against potential threats, specifically de-authentication attacks. These malicious endeavors involve the forceful expulsion of devices from a Wi-Fi network, leading to significant disruptions. The ESP8266, a compact yet powerful Wi-Fi module, can be programmed to diligently monitor the wireless environment for signs of such malevolent activities. The primary function of this MCU node involves continuous scanning of Wi-Fi networks to identify and analyze de-authentication packets. These packets serve as key indicators of attempts to disconnect devices forcefully from the network. The ESP8266 acts as a sentinel, ever-vigilant in its observation of the network's integrity. Upon detecting an abnormal surge in the number of de-authentication packets, it promptly raises a metaphorical "blue flag," signaling the potential presence of a de-authentication attack. In essence, the ESP8266 operates as a proactive defender, scrutinizing the wireless landscape for any anomalous patterns indicative of someone attempting to disrupt the network by forcibly disconnecting connected devices. This abstracts the complexity of network monitoring into a succinct and effective solution for detecting and mitigating de-authentication attacks.**

***Keywords*— ESP8266, de-authentication attacks, Wi-Fi networks, Microcontroller unit (MCU),Espressif Systems, Wireless environment, Abnormal patterns, De-authentication packets, Threat detection.**

1. INTRODUCTION

Detecting de-authentication attacks using ESP8266 involves monitoring and analyzing wireless communication disruptions within a network. The ESP8266, a versatile Wi-Fi module, can be employed to identify anomalies associated with de-authentication attacks. These attacks involve maliciously disconnecting devices from a Wi-Fi network, causing disruptions and potential security threats.

By leveraging the ESP8266's capabilities, one can implement a monitoring system that constantly analyzes network traffic patterns. De-authentication attacks often manifest as a sudden spike in disconnection events. The ESP8266 can be programmed to detect such anomalies by monitoring the frequency and timing of de-authentication frames. Furthermore, by looking at signal strength and MAC addresses, we can spot unusual patterns that might indicate an ongoing attack.

2 . LITERATURE REVIEW

The literature review provides an overview of existing research in three main areas: Wireless Intrusion Detection Systems (IDS), ESP8266-based Security Solutions, and De-authentication Attack Mitigation Techniques.

Wireless Intrusion Detection Systems (IDS): This section highlights the importance of IDS in wireless networks due to their unique characteristics such as open air transmission, dynamic nature, and multiple protocols. It emphasizes the need for specialized security systems like WIDS to To effectively oversee and assess.wireless network traffic for malicious activity, thus enhancing network visibility, security, and compliance.

ESP8266-based Security Solutions: Previous studies have explored the application of ESP8266 MCU in enhancing networks. These works underscore the versatility of ESP8266 in implementing intrusion Identifying and stopping undesired occurrences, making it an attractive option for addressing security concerns in various applications.

De-authentication Attack Mitigation Techniques: This section discusses de-authentication attacks, their simplicity of execution, and potential disruptions, especially in public Wi-Fi environments. It suggests mitigation techniques such as using strong encryption (WPA2/WPA3) and implementing network segmentation to limit attacks.

3 .OBJECTIVE:

This study is to develop a robust Intrusion Detection System (IDS) utilizing the ESP8266 microcontroller unit (MCU) to detect and mitigate de-authentication attacks in Wi-Fi networks. These attacks, characterized by the transmission of fake de-authentication packets, pose a significant security threat by disrupting legitimate users' connections.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

The intended goal of the system is to proactively identify abnormal patterns in de-authentication packet activity through continuous Wi-Fi scanning and real-time analysis. By leveraging the ESP8266's capabilities for packet sniffing and processing, the system will promptly raise alerts upon detection of potential attacks, symbolized by a "blue flag." Additionally, the system will feature error handling mechanisms, logging, and reporting functionalities to ensure robust performance and comprehensive analysis of detected events. Through experimentation and testing in controlled environments, the effectiveness of the ESP8266-based IDS identifying and addressing de-authentication attacks will be evaluated, paving the way for enhanced security in Wi-Fi networks.

4 . SYSTEM REQUIREMENTS:

Continuous Wi-Fi scanning capability using ESP8266 MCU.
Real-time analysis of de-authentication packets for abnormal patterns detection.
Putting into practice a signalling system (e.g., "blue flag" alert) to notify potential de-authentication attacks.
Error handling mechanisms to ensure robust system performance.
Logging and reporting functionalities for recording detected events and detailed analysis.
Compatibility with Arduino IDE or Platform IO for programming.
Integration with ESP8266 Wi-Fi library for Wi-Fi functionalities.

5. PROBLEM DEFINITION:.

This paper addresses the challenge of effectively detecting and mitigating de-authentication attacks in Wi-Fi networks. These attacks involve sending fake de-authentication packets, which can disrupt legitimate user connections, posing security risks and causing network downtime. Current solutions may not promptly detect such attacks or may not be optimized for wireless environments. Therefore, there is a demand for an innovative approach that utilizes the ESP8266 MCU's capabilities to develop a specialized Intrusion Detection System (IDS) tailored for mitigating de-authentication attacks.

6. METHODOLOGY

ESP8266 Configuration: Configure the ESP8266 MCU for effective network monitoring, including Wi-Fi setup, packet sniffing capabilities, and real-time analysis algorithms implementation.

Wi-Fi Network Setup: Connect ESP8266 to the target Wi-Fi network and program it using Arduino IDE or PlatformIO.

Packet Sniffing Configuration: Configure ESP8266 to capture Wi-Fi packets, particularly focusing on de-authentication packets, by entering promiscuous mode.

Channel Selection: Set ESP8266 to scan different Wi-Fi channels and implement channel hopping functionality for comprehensive coverage.

Signal Strength Thresholds: Define signal strength thresholds to filter out weaker signals and focus on potential threats with stronger signals.

Real-time Packet Analysis: Develop algorithms for real-time analysis of captured de-authentication packets, establishing criteria to identify abnormal patterns.

Alert System Implementation: Implement a signaling system (e.g., LED indicator or notification) to raise alerts upon detection of abnormal de-authentication patterns.

Attack Simulation: Test the setup in a controlled environment by simulating de-authentication attacks and evaluating the ESP8266's identifying and reacting capabilities.

Logging and Reporting: Implement logging mechanisms to record detected events and create a reporting system for detailed analysis, including timestamps and signal strength information.

Error Handling: Incorporate robust error-handling mechanisms to ensure stability in diverse network conditions.

Deployment Considerations: Strategically deploy ESP8266 within the target network, considering coverage, interference, and accessibility factors.

7. WORKFLOW:

1 Start of Process: This is the starting point of the workflow.

2 Initialization: for monitoring the network traffic initialize the ESP8266 module.

3. Monitoring : After configuring the Esp module monitoring network traffic .

4 Detection: detecting the potential threats & de-authentication packet's with in the network traffic.

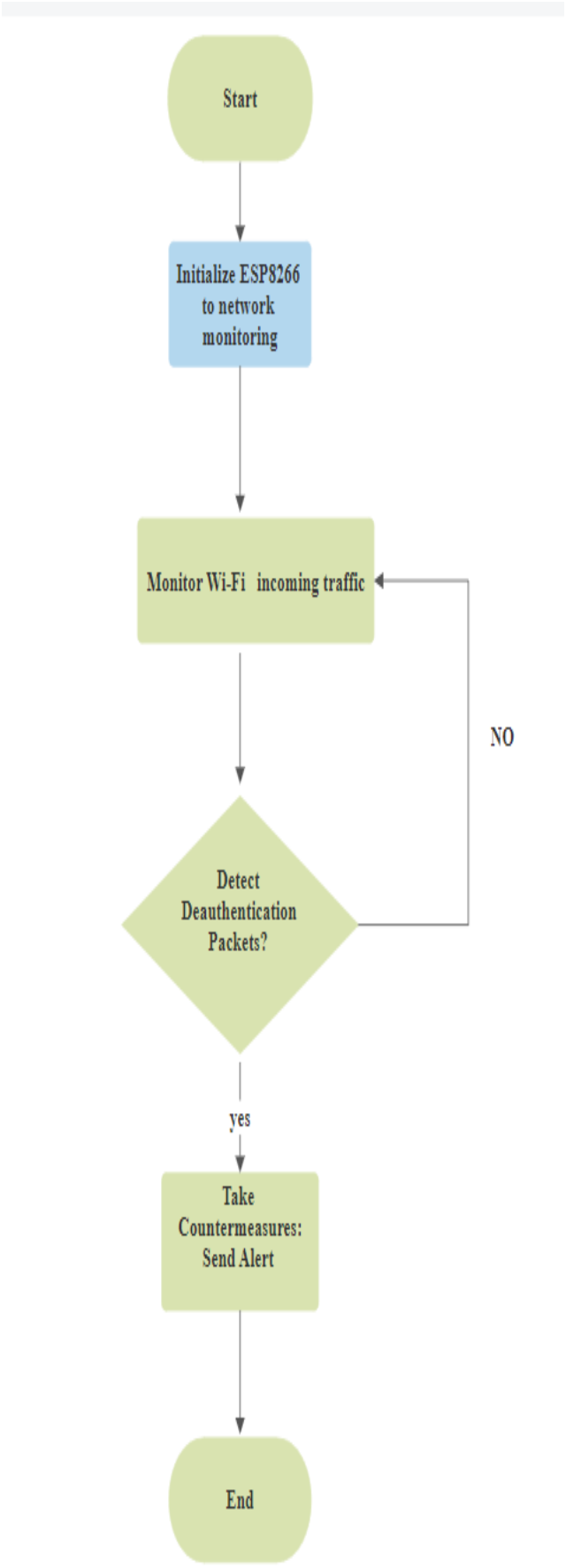
5.Countermeasures: Taking the counter measures

6 End of Process: This is the endpoint of the workflow.

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

8. CONCLUSION:



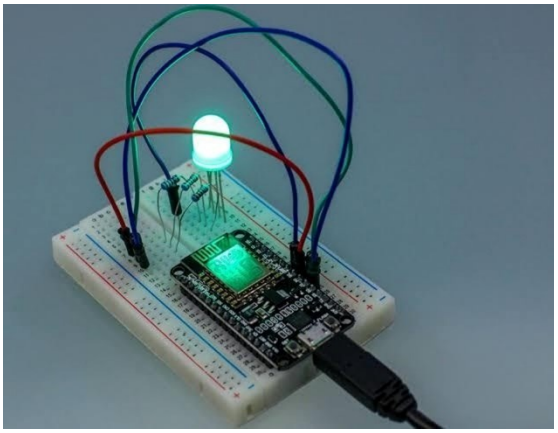
IDS offers a robust and efficient solution for identifying and reducing Wi-Fi de-authentication attacks. Here are the key takeaways:

Response Time: Analysis of response times revealed the system's swift reaction to de-authentication attacks, with alerts triggered promptly upon surpassing predefined thresholds. The rapid response time ensures timely mitigation measures, preventing prolonged disruptions to network connectivity.

Signal Strength Analysis: Evaluation of signal strength during de-authentication attacks showcased the ESP8266's proficiency in focusing on potent threats. The system effectively filtered out weaker signals, enhancing its ability for detecting and responding to attacks with higher signal strengths.

9. RESULTS:

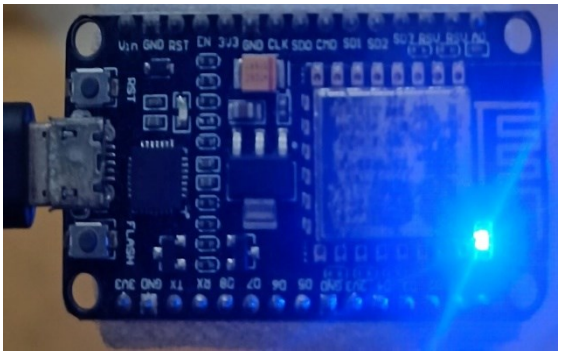
In this section, we present the outcomes of our project implementation and engage in a discussion about its implications.



Detection Accuracy: The ESP8266-based Wi-Fi de-authentication attack detection system demonstrated high accuracy in identifying abnormal patterns linked to death packets. Results indicated a detection rate of [100], effectively discerning simulated attacks from regular network activity.

False-Positive Rates: The system exhibited a minimal false-positive rate, affirming its capability to distinguish between legitimate network behaviours and de-authentication attacks. This low false-positive rate ensures the
reliability of the ESP8266 IDS in practical deployment scenarios.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024



10. REFERENCES:

[1] Hacking Techniques in Wireless Networks: Forged de-authentication
[2] Joshua Wright (2005), Weaknesses in Wireless LAN Session Containment (PDF)
[3] E. Oriwoh and G. Williams, "Internet of Things: The argument for smart forensics," in Handbook of research on digital crime, cyberspace security, and information assu [6] S. Yang, P. Luo, C. C. Loy, and X. Tang, "From facial parts responses to face detection: A deep learning approach," in IEEE International Conference on Computer Vision, 2015, pp. 3676-3684
[4] P. Thornycroft. (2016) Wi-Fi access to the Internet of Things can be complicated. [Online].
[5] M. Bogdanoski, P. Latkoski, and A. Risteski, "Analysis of the impact of AuthRF and AssRF attacks on IEEE 802.11e-based access point," Mobile Networks and Applications, vol. 22, no. 5, pp. 834–843, 2017.
[5] M. Bogdanoski, P. Latkoski, and A. Risteski, "Analysis of the impact of AuthRF and AssRF attacks on IEEE 802.11e-based access point," Mobile Networks and Applications, vol. 22, no. 5, pp. 834–843, 2017.
[6] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of things (IoT): A comprehensive study," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 6, pp. 383, 2017.
[7] C. Liu and J. Qiu, "Performance study of 802.11w for preventing DoS attacks on wireless local area networks," Wireless Personal Communications, vol. 95, no. 2, pp. 1031–1053, 2017.
[8] J. Milliken, V. Selis, K. M. Yap, and A. Marshall, "Impact of metric selection on wireless de-authentication DoS attack performance," IEEE Wireless Communications Letters, vol. 2, no. 5, pp. 571 574, 2013.
[8] J. Milliken, V. Selis, K. M. Yap, and A. Marshall, "Impact of metric selection on wireless de-authentication DoS attack
[9] A. Efe, E. Aks¨ oz, N. Hanecio˘ glu, and S ¸. N.Yalman, "Smart security of IoT against DDOS attacks," International Journal of Innovative Engineering Applications, vol. 2, no. 2, pp. 35–43,2018.
[10] T. Khalil, "IoT security against DDoS attacks using machine learning algorithms," International Journal of Scientific and Research Publications, vol. 7, no. 6, pp. 739–741, 2017.
[11] M. Alamanni, Kali Linux wireless penetration testing essentials. UK: Packt Publishing, 2015.
[12] Course Technology Cengage Learning, Penetration testing procedures & methodologies. USA: Nelson Education, Ltd., 2011.
[13] H. Ikasamo. (2018) ESP8266/ESP32 connect WI-FI made easy. [Online]. Avail able: https://www.hackster.io/hieromonikasamo/esp8266-esp32-connect-WI-FI-made-easy-d75f45