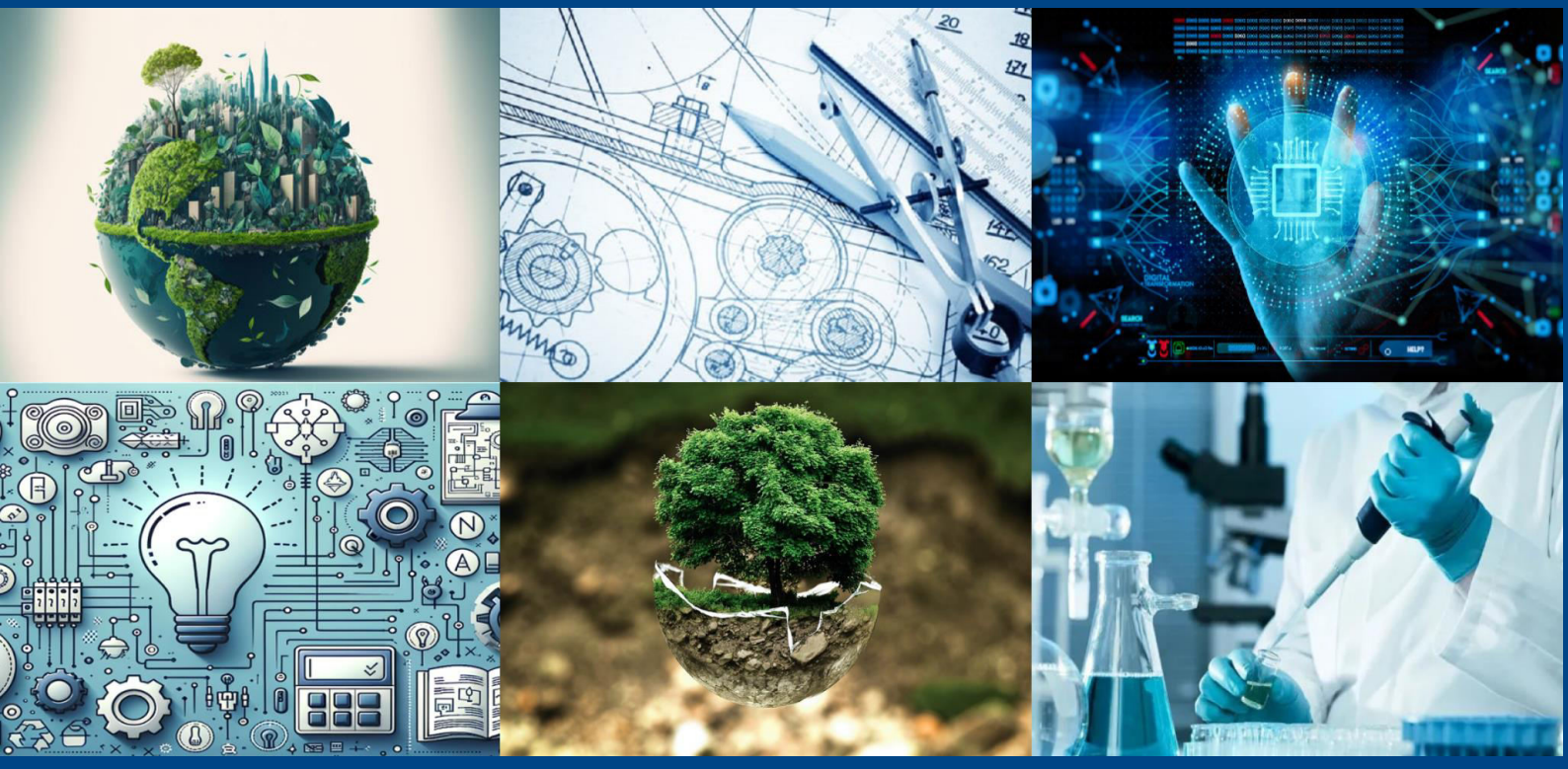
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 5, May 2025**

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805253

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Deauther using IOT

Nandhini K V, Dr.Vishwa Priya

Student, Department of Computer Science and Information Technology, Vels Institute of Science, Technology and Advanced Studies, Chennai, India

Assistant Professor, Department of Computer Science and Information Technology, Vels Institute of Science, Technology and Advanced Studies, Chennai, India

ABSTRACT: This project presents the development of a compact and portable Wi-Fi Deauther device using the NodeMCU ESP8266 micro controller. The system leverages an OLED display for real-time status updates and user interaction. A rechargeable lithium-ion battery, managed by a TP4056 charging module, provides standalone power with boot-up functionality. The components are assembled on a dot PCB board to ensure durability and ease of assembly. A push button is integrated for user control, enabling the execution of specific deauthentication attacks on selected Wi-Fi networks. This device serves educational and testing purposes, demonstrating the vulnerabilities in Wi-Fi security protocols (specifically 802.11) by performing deauthentication frame attacks. It highlights the importance of network protection and ethical usage in cybersecurity.

I. INTRODUCTION

The advancement of wireless communication and the increasing adoption of Internet of Things (IoT) devices have significantly improved the way we live, work, and interact with technology. Smart homes, industrial automation, healthcare monitoring, and agricultural systems now depend heavily on Wi-Fi networks to connect and communicate. However, this dependence has also introduced a growing number of security threats. As more devices connect to the internet, ensuring the security of wireless networks becomes a critical concern.

One of the common vulnerabilities in Wi-Fi networks is the deauthentication attack. This type of attack exploits a flaw in the Wi-Fi protocol, where unencrypted deauthentication packets can be sent to force a device to disconnect from the network. These packets do not require any encryption or authentication, which makes them a significant point of weakness. The concept of a Deauther arises from this vulnerability—it is a tool or device capable of sending such packets to disrupt network connectivity intentionally.The goal of this project is to develop a Deauther using IoT, which not only demonstrates the attack mechanism but also incorporates smart control and monitoring through an internet-based platform. By utilizing an IoT-capable microcontroller like the ESP8266, the system becomes accessible remotely and can be used in real-time testing and demonstrations. This approach is valuable for educational purposes, cybersecurity training, and ethical hacking practices aimed at strengthening Wi-Fi security.

The Deauther system utilizes the ESP8266 NodeMCU, a compact and cost-effective microcontroller that includes built-in Wi-Fi capabilities. The firmware on the ESP8266 is programmed to scan for Wi-Fi networks and connected clients. Once the targets are identified, users can send deauthentication packets to any client or access point, forcing them to disconnect from the network.To make the system IoT-enabled, a web dashboard or mobile app is integrated using platforms such as Blynk, Firebase, or a custom HTTP interface. This allows users to operate the deauther remotely, visualize connected devices, and select targets from a simple graphical interface. Additional features such as an OLED display can be added to show status updates and signal strength in real time.

II. LITERATURE REVIEW

The IEEE 802.11 protocol, which defines the standard for wireless local area networks (WLANs), includes a deauthentication frame used to manage device disconnection from an access point (AP). While functional in design, this frame is unencrypted and unauthenticated, making it vulnerable to exploitation. Research by Bellardo and Savage (2003) demonstrated that deauthentication packets can be spoofed easily, allowing attackers to forcibly disconnect users from a wireless network without needing access credentials.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805253

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Several studies have since addressed this weakness. F. Ahmad et al. (2017) emphasized that even networks protected by WPA2 encryption are susceptible to deauthentication attacks, which exploit the management frames before any encryption occurs. These attacks are classified as Denial of Service (DoS) attacks and can lead to serious network disruptions.

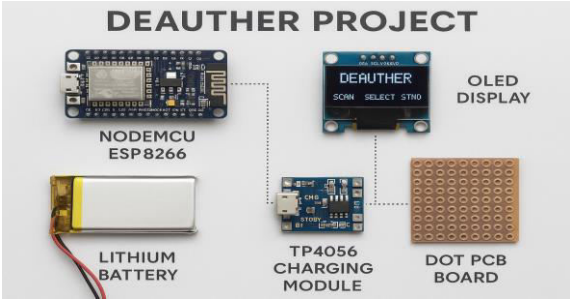


FIGURE 1

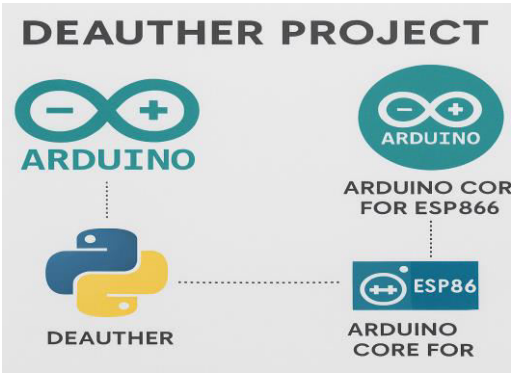


FIGURE 2

III. METHODOLOGY

The **802.11 Wi-Fi protocol** includes management frames such as **beacon, probe, authentication, association, disassociation, and deauthentication frames**. These frames are **unencrypted** even in secure networks (WPA/WPA2/WPA3), because they are exchanged **before** encryption is negotiated. A **deauthentication frame** is normally used by either the access point (AP) or the client to signal the end of a session.In a **Deauthentication Attack**, an attacker **spoofs** these frames—pretending to be the AP—and sends them to connected clients. As a result, clients believe they are being kicked off the network, and they disconnect. If this is repeated continuously, the device is effectively **denied service (DoS)**.Wi-Fi uses **management frames** to maintain communication.A **deauthentication frame** is a legitimate signal sent when a device disconnects from a network.Attackers spoof these frames to force devices to disconnect. A **Deauther using IoT** is a technique that utilizes small Wi-Fi-enabled microcontrollers like the **ESP8266** or **ESP32** to exploit vulnerabilities in the **IEEE 802.11 Wi-Fi protocol**, specifically targeting unencrypted management frames such as **deauthentication** and **disassociation** frames. These frames are typically used to manage connections between access points and client devices, and since they are not protected by encryption, they can be easily spoofed. By flashing custom firmware—such as the popular open-source **ESP8266 Deauther** developed by Spacehuhn—onto an ESP device, it can be programmed to scan for nearby Wi-Fi networks, identify connected clients, and send forged deauthentication packets. These packets trick devices into believing they've been disconnected by the network, resulting in a **denial-of-service (DoS)** as users are repeatedly kicked off and unable to maintain a connection. The ESP device can also host a local web interface, allowing attackers to control the deauth operation through a browser by selecting target networks and clients. Additionally, advanced features like **beacon flooding** and **probe request spamming** can be used to confuse nearby devices or flood Wi-Fi lists with fake networks. While powerful for penetration testing and educational purposes, this methodology is considered illegal if used without explicit permission, as it disrupts legitimate network communication and violates wireless communication regulations.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805253

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. RESULTS AND DISCUSSIONS

The implementation of a **Deauther using IoT**, particularly with an ESP8266 or ESP32, demonstrates a highly effective yet simple method of conducting **Wi-Fi denial-of-service (DoS)** attacks by exploiting weaknesses in the 802.11 protocol. During testing in a controlled environment, the deauther was able to successfully scan and detect multiple nearby Wi-Fi access points and the clients connected to them. Once targets were selected, the ESP8266 sent forged **deauthentication frames**, effectively disconnecting devices from their networks within seconds. This validated the device's ability to perform packet injection and spoof MAC addresses, confirming the vulnerability of unprotected management frames in even WPA2-secured networks. Additionally, features like **beacon flooding** resulted in the creation of numerous fake Wi-Fi SSIDs, which cluttered the available network list on nearby devices and slowed down their ability to connect to legitimate networks. However, the effectiveness of the attack varied depending on signal strength, client device behavior (some auto-reconnect faster than others), and router configurations—some modern routers can detect and ignore excessive deauth frames. The results highlight the need for stronger encryption and authentication of management frames, such as the implementation of **802.11w Protected Management Frames (PMF)**, to mitigate such attacks. From a discussion standpoint, while the deauther tool proves valuable for educational and ethical hacking scenarios, it also emphasizes the ethical risks and potential for abuse, especially considering the low cost, ease of use, and minimal technical skill required to launch disruptive attacks. As such, it underscores the importance of educating users, IT professionals, and network administrators about securing wireless networks and enforcing legal frameworks to prevent misuse.

V. CONCLUSION

In conclusion, the development and deployment of a **Deauther using IoT**—particularly through microcontrollers like the **ESP8266** or **ESP32**—demonstrates both the power and vulnerability inherent in modern wireless communication protocols. This project effectively reveals how unencrypted management frames within the **IEEE 802.11 Wi-Fi standard**can be exploited to disrupt network connectivity through the injection of forged deauthentication packets. The experiment confirmed that with minimal hardware and technical setup, one can create a highly effective denial-of-service (DoS) attack that disconnects clients from Wi-Fi networks and renders them unable to reconnect during the course of the attack. Furthermore, the inclusion of additional features such as beacon flooding and probe request spamming illustrates the broader scope of disruption possible through simple IoT-based devices. While this tool has legitimate uses in **penetration testing, cybersecurity education**, and **network vulnerability assessment**, its ease of use and accessibility also raise serious **ethical and legal concerns**. The study reinforces the urgent need for widespread adoption of **Protected Management Frames (802.11w)** and other wireless security enhancements to safeguard against such exploits. Ultimately, this project not only highlights a critical flaw in wireless communication but also serves as a reminder of the dual-edged nature of technological advancement—capable of both securing and subverting the systems we rely on every day.

REFERENCES

1. Raj, P., & Raman, A. (2017). The Internet of Things: Enabling Technologies, Platforms, and Use Cases. CRC Press.
2. Shilpa, S., & Ranjitha, R. (2021). "IoT Based Smart Agriculture Monitoring System," International Journal of Engineering Research & Technology (IJERT), Vol. 10, Issue 06.
3. Ahmed, S. (2020). "IoT Based Flood Monitoring and Alerting System Using NodeMCU," International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Vol. 9, Issue 3.
4. Blynk IoT Platform Documentation. (2023). https://docs.blynk.io
5. NodeMCU Documentation. (2022). https://nodemcu.readthedocs.io
6. Sharma, D., & Patel, M. (2019). "Smart Water Level Monitoring System Using IoT," International Research Journal of Engineering and Technology (IRJET), Vol. 6, Issue 2.
7. ESP8266 Official Documentation. (2023). Espressif Systems. https://www.espressif.com/en/products/socs/esp8266
8. Open Source Deauther Project. (2023). SpacehuhnTech. https://github.com/SpacehuhnTech/esp8266_deauther
9. Kumar, V., & Singh, A. (2020). "Wireless Sensor Network-Based Smart Farming," IEEE International Conference on Smart IoT Systems, pp. 45–50.
10. Al-Fuqaha, A., et al. (2015). "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, Vol. 17, No. 4, pp. 2347–2376.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com