Project Report: ESP8266 Wi-Fi Deauther

---

1. Introduction

The **ESP8266 Wi-Fi Deauther** is a portable device built using the **NodeMCU ESP8266 V3 Lua CH340** microcontroller. It is powered by a **3.7V lithium battery** and uses a **5V Step-Up Power Module** for stable power delivery. The device is controlled via a web interface and can perform Wi-Fi deauthentication attacks, beacon spam, and probe request floods. This project is designed for educational purposes and ethical security testing.

---

2. Objectives

- To build a portable Wi-Fi deauther using the **NodeMCU ESP8266**.
- To power the device using a **3.7V lithium battery** and a **5V Step-Up Power Module**.
- To create a compact, screenless device controlled via a web interface.
- To understand Wi-Fi vulnerabilities and ethical hacking concepts.

---

3. Components Used

1. **NodeMCU ESP8266 V3 Lua CH340**
    - The main microcontroller with built-in Wi-Fi capabilities.
2. **5V Step-Up Power Module (134N3P)**
    - Converts the 3.7V battery voltage to a stable 5V output for the NodeMCU.
    - Includes lithium battery charging and protection features.
3. **3.7V Lithium Battery (200mAh)**
    - Provides portable power to the device.
4. **On-Off Button Switch**
    - Used to power the device on and off.
5. **Resistor**
    - Manages power delivery to the NodeMCU.
6. **Wires**
    - For connecting all components.
7. **Enclosure**
    - A box to house all components securely.

---

4. Software and Tools

1. **Precompiled Deauther Firmware**
    - Downloaded from deauther.com.

2. **ESP Web Tool**
    - Used to flash the `.bin` firmware onto the NodeMCU.
    - Accessed via esp.huhn.me.
3. **Web Browser**
    - To access the Deauther web interface and control the device.

---

5. Steps to Build the Project

Step 1: Gather Components

- Ensure you have all the components listed above.

Step 2: Connect the Hardware

1. **Connect the Battery**
    - Attach the **3.7V lithium battery** to the **5V Step-Up Power Module** using the battery connector.
2. **Connect the NodeMCU**
    - Use a USB cable to connect the **5V Step-Up Power Module's USB-A output** to the **NodeMCU's Micro-USB port**.
3. **Add the On-Off Switch**
    - Wire the **on-off button switch** between the battery and the power module to control power delivery.
4. **Add a Resistor**
    - Use a resistor to manage the power flow and prevent overloading the NodeMCU.
5. **Pack Everything**
    - Place all components inside the enclosure for a clean and portable design.

Step 3: Flash the Firmware

1. Download the **Deauther `.bin` file** from deauther.com.
2. Open the **ESP Web Tool** in a supported browser: esp.huhn.me.
3. Connect the NodeMCU to your computer via USB.
4. Click **Connect** and select the correct serial port.
5. Upload the `.bin` file and click **Program**.
6. Wait for the flashing process to complete.

Step 4: Access the Web Interface

1. After flashing, the NodeMCU will create a Wi-Fi access point (AP) named `pwned`.
2. Connect to this AP using the default password `deauther`.
3. Open a web browser and navigate to `192.168.4.1` to access the Deauther web interface.

Step 5: Perform Actions

1. **Scan for Networks**
    - Use the web interface to scan for nearby Wi-Fi networks.
2. **Select a Target**
    - Choose a network or device from the scan results.
3. **Launch Attacks**
    - Perform deauthentication attacks, beacon spam, or probe request floods.

---

6. Features

1. **Portable Design**

    - Powered by a 3.7V lithium battery and housed in a compact enclosure.
2. **Web Interface**
    - Controlled via a browser on any Wi-Fi-enabled device.
3. **Deauthentication Attacks**
    - Disconnects devices from a target Wi-Fi network.
4. **Beacon Spam**
    - Creates fake Wi-Fi networks to confuse or overwhelm devices.
5. **Probe Request Flood**
    - Sends a flood of probe requests to detect hidden networks.

---

7. Applications

- **Wi-Fi Security Testing**
    - Test the resilience of your own Wi-Fi network against deauthentication attacks.
- **Educational Tool**
    - Learn about Wi-Fi vulnerabilities and network security.
- **Penetration Testing**
    - Use in authorized penetration testing scenarios to identify network weaknesses.

---

8. Ethical and Legal Considerations

- **Legal Use**
    - Only use this tool on networks you own or have explicit permission to test. Unauthorized use is illegal.
- **Ethical Use**
    - This project is intended for educational purposes and security research. Misuse can lead to legal consequences.
- **Disclosure**
    - Always inform network owners before testing their networks.

---

9. Limitations

- **Wi-Fi Only**
    - The ESP8266 cannot perform attacks on 4G or other types of networks.
- **Range**
    - The effective range is limited to the Wi-Fi signal strength of the ESP8266.
- **Battery Life**
    - A 200mAh battery may provide limited runtime; consider using a higher-capacity battery for longer use.

---

10. Future Enhancements

1. **Higher Capacity Battery**
    - Use a larger battery (e.g., 1000mAh) for extended runtime.
2. **External Antenna**
    - Add an external antenna to improve Wi-Fi range.
3. **Advanced Attacks**
    - Implement more advanced Wi-Fi attacks, such as Evil Twin or WPA2 cracking (requires additional hardware).
4. **Cloud Integration**
    - Use cloud services like Blynk or MQTT for remote control over the internet.

---

11. Conclusion

The **ESP8266 Wi-Fi Deauther** is a powerful and portable tool for understanding Wi-Fi security vulnerabilities. By following this project, you've built a compact, screenless device that can perform deauthentication attacks and other Wi-Fi-related actions. Always use this tool responsibly and only in authorized scenarios.

12. References

1. Deauther Official Website
2. ESP Web Tool
3. NodeMCU ESP8266 Documentation