Wi-Fi Deauthentication Attack Simulator (Safe, Non-Transmitting)

Overview:
This project is an **educational cybersecurity simulator** built with the NodeMCU ESP8266 and a 0.96” OLED screen. It **does not transmit or interfere** with any Wi-Fi networks. Instead, it **scans nearby networks**, automatically selects the strongest SSID, and runs a **timed simulation** of a Wi-Fi deauthentication attack, showing progress on the OLED and logging to serial.

Key Features

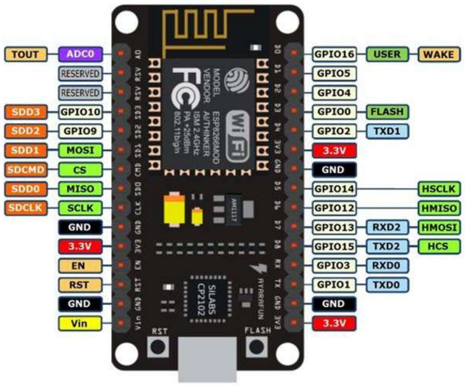
- Wi-Fi scanning with auto-selection of the strongest access point (SSID).
- OLED-based user interface with centered text and live progress bar.
- Simulation timer (2–5 minutes) with countdown display.
- Serial log output simulating deauthentication packet sending (without transmission).
- Safe, legal, and ethical demonstration of Wi-Fi attack concepts.

Technical Details

Hardware: NodeMCU ESP8266 (LoLin) + 0.96” SPI OLED display.
Libraries: ESP8266WiFi, Adafruit_GFX, Adafruit_SSD1306.
Languages: C++ (Arduino).
Wiring: SDA→D7, SCL→D5, RST→D3, DC→D8.
Output: OLED progress screens + Serial logs.

Visual References:

Below is a labeled NodeMCU ESP8266 and SPI OLED display pinout diagram, which helps explain the wiring connections used in this project.



Educational Value

This project is designed to **teach wireless security concepts responsibly**. It helps to **visualize how a Wi-Fi deauthentication attack works** without performing any malicious transmissions. Such a demonstration highlights the **importance of cybersecurity awareness** and showcases embedded systems programming skills.

Portfolio Relevance:
This project demonstrates knowledge of **IoT devices, wireless communication, user interface design, and cybersecurity simulation**.