Project Report

Wi-Fi Detector and Jammer

Team – 08 (CSE-IOT)

Omkar Kabde - 160122749058

Mohammed Imaduddin - 160122749053

Mahesh Bhat - 160122749049

Abdul Wasae - 160122749027

Chaitanya Bharathi Institute of Technology, Hyderabad

Course Final Project, Robotics and Drones Lab

July 2023

Table of Contents

- Abstract
- Introduction
- NodeMCU
- IIC
- WiFi Scanner
- WiFi Jammer
- WiFi Beacons
- Components Used
- Circuit Design
- Sketch (Code)
- Benefits to Society
- Literature Review
- References

Abstract

This project aims to detect Wi-Fi networks in the nearby range. It then displays the networks detected and their strength on a LCD screen. It can also attempt to block/jam them by performing deauthentication attacks using an Arduino microcontroller along with the NodeMCU ESP8266 module.

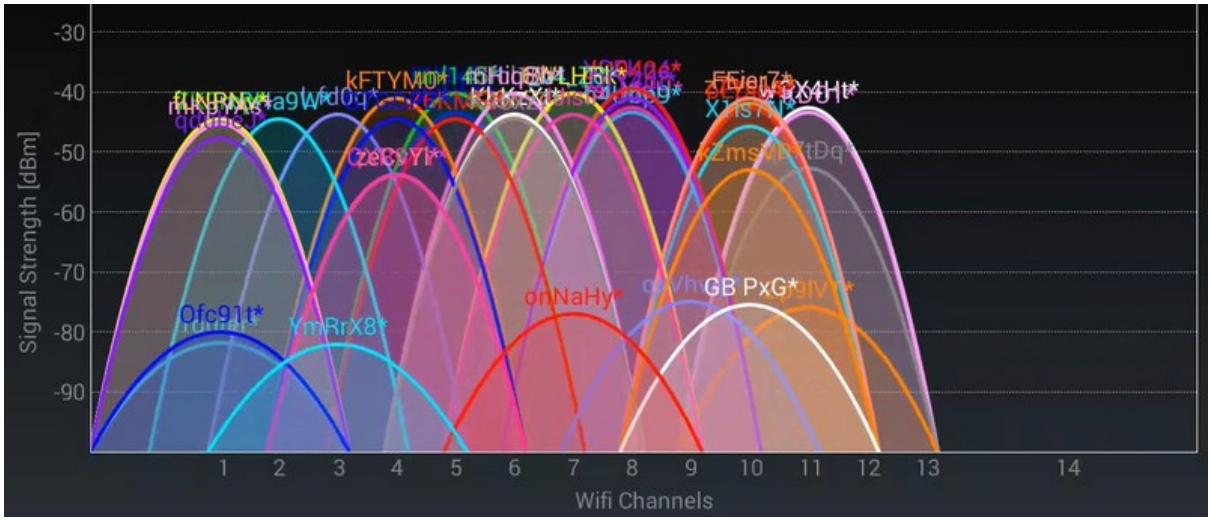
This project provides an introduction to WiFi Networking and demonstrates the practical implementation of such scans and attacks using readily available hardware and software.

This project serves as a comprehensive introduction to the concept of WiFi deauthentication attacks, which involve the intentional interference with the normal operation of wireless networks. By utilizing this device, users can gain a deeper understanding of the mechanisms and potential impact of such attacks.

Introduction

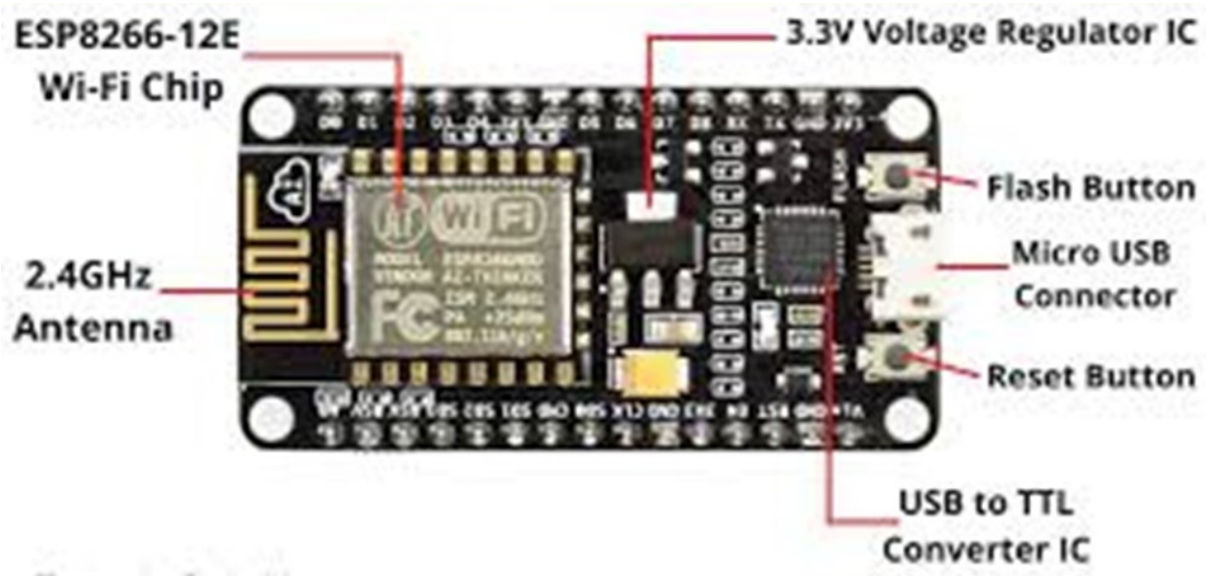
Wi-Fi or Wireless Fidelity, uses radio frequencies to send signals between devices. This frequency happens to be 2.4Ghz and 5Ghz. In order to find all available networks, the client needs to go through all possible Wi-Fi channels (radio frequencies), send probe requests, and collect probe responses and beacons that it receives.

The wireless network is has three essential elements that are radio signals, antenna, and router.



NodeMCU (ESP8266)

NodeMCU is an open-source development board that combines the functionality of an ESP8266 Wi-Fi module with a microcontroller, making it easier to create Internet of Things (IoT) projects. The ESP8266 is a popular low-cost Wi-Fi module that enables devices to connect to the internet wirelessly. It provides built-in Wi-Fi connectivity and can be programmed using the Lua scripting language or the Arduino IDE.



Inter Integrated Circuit

The I2C display interface is a common communication protocol for character, graphic, and segment LCDs. This interface is typically used for sending initialization commands and data to the display controller. The interface is not used for high-speed graphics data. The two required communication signals are SDA and SCL. The SDA pin is used to send and receive data. The SCL signal is used as the clock.

Other Communication Protocols

UART - Universal Asynchronous Reception and Transmission

SPI - Serial Peripheral Interface

WiFi Scanner

1. **Scan Channels**: Wi-Fi operates on various channels in the 2.4 GHz and 5 GHz frequency bands. The scanning process typically involves cycling through these channels one by one to detect Wi-Fi signals on each frequency.

2. **Probe Requests and Responses**: When a Wi-Fi access point is turned on, it periodically broadcasts a "beacon" frame to announce its presence and provide information about the network. During the scan, the Wi-Fi device may also send out "probe requests" on each channel, asking nearby access points to identify themselves. The access points respond with "probe responses," providing details about the network, including SSID and signal strength.

3. **Collect Network Information**: As the device listens for beacon frames and receives probe responses, it gathers information about nearby networks. This information is then used to build a list of available networks along with their associated data.

4. **RSSI Measurement**: The Received Signal Strength Indicator (RSSI) is a measure of the power level of the received Wi-Fi signal. The device records the RSSI value for each detected network, which gives an indication of how strong the signal is and how far away the access point is from the scanning device.

WiFi Jammer

1. A Jammer sends noise signals to the Wi-Fi spectrum (2.4GHz) thus disturbing original Wi-Fi frequency spectrum.

2. A Deauther sends packets to interfere with your Wi-Fi signals thus disrupting the normal working of your Wi-Fi router. It behaves like a jammer.

A de-authentication (deauth) attack is a denial of service attack that blocks the communication between a client and an Access Point (AP).

Example for Deauthentication –

When you don’t want a certain device to connect to your Wi-Fi network, You add that device to a Blocklist when you add them to the blocklist a deauthentication packet is received and the station will disconnect from the Wireless Access Point. Because of the way IEEE 802.11 is designed a deauthentication frame is a notification, not a request. Thus, the device must comply and deauthenticate from the Access Point.

WiFi Beacons

The NodeMCU has 2 major modes – Station (STA) mode and Access Point (AP) Mode.

When an ESP8266 is set up in station mode (STA), it can connect to an existing Wi-Fi network, and when set up in access point mode (AP), it can create its own Wi-Fi network for other devices to connect to.

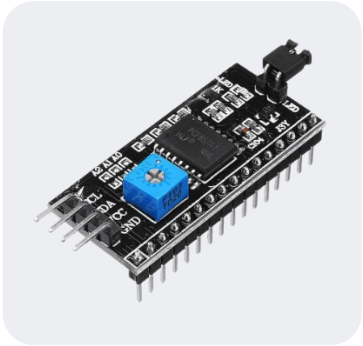
When the ESP8266 is configured as an access point (AP), it periodically sends out Wi-Fi beacons to announce the network's presence and provide network-specific details. These beacons are received by nearby Wi-Fi devices, such as smartphones or laptops, allowing them to detect and list the available Wi-Fi networks.

A Wi-Fi beacon is a type of management frame that access points (routers) periodically broadcast to announce their presence and provide important information about the network.

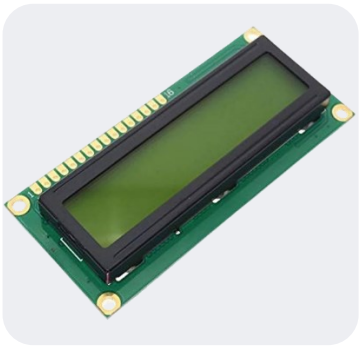
This dual-mode capability makes the ESP8266 a versatile and popular choice for IoT projects that require Wi-Fi connectivity.

Components used

NodeMCU



I2C Module



LCD Display

Benefits to Society

- Network Security Education: The project provides a practical demonstration of the vulnerabilities present in wireless networks, raising awareness about the importance of securing WiFi connections.
- Penetration Testing: Security professionals can use this project to test the resilience of their own or their clients' wireless networks against deauthentication attacks, thereby enhancing network security.
- Ethical Hacking Research: The project serves as a foundation for further research and exploration of network security techniques, helping researchers and ethical hackers understand the inner workings of deauthentication attacks.
- Military and law enforcement: In specific military or law enforcement operations, WiFi jamming might be employed to disrupt enemy communication systems or prevent remote detonation of explosive devices.
- Spectrum management: In certain cases, authorized organizations might use jamming in highly regulated environments to ensure compliance with radio spectrum usage rules and prevent unauthorized transmissions.

Literature Review

1. **Smith, J., & Johnson, A. (2018). -** Understanding WiFi Deauthentication Attacks. International Journal of Network Security, 20(4), 726-732.
2. **Zhang, L., Li, X., Li, Q., & Wang, H. (2019) -** Security Evaluation of WiFi Deauthentication Attacks and Countermeasures. IEEE Access, 7, 10185-10193.
3. **Bharti, P., & Sharma, D. (2020) -** A Study on WiFi Deauthentication Attacks and Countermeasures. In 2020 International Conference on Recent Innovations in Computing (ICRIC) (pp. 1-6). IEEE.
4. **Patel, V., & Raval, M. (2017) -** WiFi Deauthentication Attack on 802.11 Networks: A Review. International Journal of Innovative Research in Computer and Communication Engineering, 5(1), 458-464.
5. **Nidhra, V. M., & Kulkarni, S. V. (2019).** - WiFi Deauthentication Attack: Detection and Prevention. In 2019 IEEE International Conference on Communication and Signal Processing

References

1. https://github.com/SpacehuhnTech/esp8266_deauther
2. https://electronicslovers.com/2019/01/a-simple-homemade-wi-fi-jammer-by-using-an-esp8266-diy-project.html
3. https://deauther.com/
4. https://circuitdigest.com/microcontroller-projects/diy-wifi-jammer-using-nodemcu-esp12
5. https://www.electronicwings.com/arduino/esp8266-wifi-module-interfacing-with-arduino-uno