To Kill Wi-Fi Using ESP-8266 Module

Ashish Vishwakarma  
ashishvk103@gmail.com  
Thakur Polytechnic, Mumbai, Maharashtra

Rohan Kamble  
r99kamble@gmail.com  
Thakur Polytechnic, Mumbai, Maharashtra

Jainam Shah  
jainam058@gmail.com  
Thakur Polytechnic, Mumbai, Maharashtra

Kalpesh Kubal  
kalpesh.co@tpoly.in  
Thakur Polytechnic, Mumbai, Maharashtra

ABSTRACT

The Aim of this paper is to create a project to kill wi-fi as in kill unwanted devices. This device main function alert people against the flaws of their routers. The heart of this board is wi-fi module esp-12E. This program code which we have developed kicks unwanted people of the wi-fi by attacking the routers and creates fake SSID’s or removes every user. This module has a powerful enough on-board processing and storage capability that allows it to be integrated with the sensors and other application specific devices through its GPIOs with minimal development up-front and minimal loading during runtime. Its high degree of on-chip integration allows for minimal external circuitry, including the front-end module, is designed to occupy minimal PCB area. So the User who’s stealing (victim) won’t understand why he got disconnected nor he’ll be able to figure who’s behind it.

Keywords— Arduino IDE, Arduino UNO, ESP-8266

1. INTRODUCTION

Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The term may also refer to the protection of the wireless network itself from adversaries seeking to damage the confidentiality, integrity, or availability of the network. The most common type is Wi-Fi security, which includes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is an old IEEE 802.11 standard from 1997. It is a notoriously weak security standard: the password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP was superseded in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP Enterprises often enforce security using a certificate-based system to authenticate the connecting device, following the standard 802.11X. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

2. Motives Behind This Project

1.1 Detection
The ESP8266 Wi-Fi Module is a self-contained SOC with integrated TCP/IP protocol stack that can give any microcontroller access to your Wi-Fi network. The ESP8266 is capable of either hosting an application or offloading all Wi-Fi networking functions from another application processor. Each ESP8266 module comes pre-programmed with an AT command set firmware, meaning, you can simply hook this up to your Arduino device and get about as much Wi-Fi-ability as a Wi-Fi Shield offers. The ESP8266 module is an extremely cost-effective board with a huge, and ever growing, community.

1.2 Scanning
This module has a powerful enough on-board processing and storage capability that allows it to be integrated with the sensors and other application specific devices through its GPIOs with minimal development up-front and minimal loading during runtime. Its
high degree of on-chip integration allows for minimal external circuitry, including the front-end module, is designed to occupy minimal PCB area. The ESP8266 supports APSD for VoIP applications and Bluetooth co-existence interfaces, it contains a self-calibrated RF allowing it to work under all operating conditions, and requires no external RF parts.

1.3 Identification
There is an almost limitless fountain of information available for the ESP8266, all of which has been provided by amazing community support. In the Documents section below you will find many resources to aid you in using the ESP8266, even instructions on how to transforming this module into an IoT (Internet of Things) solution.

1.4 Security
Security on IoT devices is paramount, especially if your device is going to be transmitting private information. But there is a catch! Security algorithms are often resource consuming and require large processing power to calculate, not typically an issue for desktop PCs or smartphones. IoT devices, however, are often based on very small microcontrollers. Even the PIC16 8-bit devices can be used as IoT devices. These devices are already limited on their ROM and RAM sizes.

1.5 Higher Vandalism
Whether you’re a home or a business owner, vandalism may be a constant threat. Vandalism is often anything from graffiti to destroying windows or the other sort of intentional property damage. This will help you full-fil your evil deeds.

![ESP8266 Wi-Fi Module](image)

Figure 1: ESP8266 Wi-Fi Module

2. CONCLUSION
We successfully learned how to develop a C++ program code for Arduino to make ESP-8266-NodeMCU Module Work. We managed to remove unwanted people off the Wi-Fi. Successfully created multiple fake SSID’s.

3. REFERENCES
[1] Arduino Repository
[3] ESP Community
[4] Little File System