International Journal of Electronics and Communication Engineering and Technology (IJECET)
Volume 10, Issue 2, March-April 2019, pp. 23-30. Article ID: IJECET_10_02_004
Available online at
http://www.iaeme.com/IJECET/issues.asp?JType=IJECET&VType=10&IType=2
ISSN Print: 0976-6464 and ISSN Online: 0976-6472
© IAEME Publication

DEAUTHENTICATION OF IP DRONES AND CAMERAS THAT OPERATE ON 802.11 WIFI STANDARDS USING ESP8266

S. Raja Gopal
Senior Member, IEEE, Department of Electronics and Communication Engineering
KL University, Vaddeswaram, Andhra Pradesh, India

P. Ranga Prasanth, S. Veerabhadra swamy, P. Sunil Krishna and R. Loshith Kumar
Members, IEEE, Department of Electronics and Communication Engineering,
KL University, Andhra Pradesh, India

ABTRACT

At present, wifi is one of the genuine prerequisites for everyone. There are a large number of SOC'S out there however ESP8266 Wi-Fi module is an independent System on-chip (SOC) with coordinated TCP/IP convention stacks that can give any microcontroller access to a Wi-Fi network. Here we deauthenticate the customer to interface with internet. The deauthentication assault, is utilized to separate gadgets from their WiFi organize. Nobody appears to think about this immense defenselessness in the authority 802.11 WiFi norms. In any case, this paper is to teach individuals to refresh there Wifi from 802.11 to 802.11w due to the powerlessness of 802.11 WiFi guidelines since it is effectively deauthenticated utilizing ESP8266.

Keywords: Wifi, Wifi Module. Deauthentication, System on Chip (SOC), ESP8266.

Cite this Article: S. Raja Gopal, P. Ranga Prasanth, S. Veerabhadra Swamy, P. Sunil Krishna and R. Loshith Kumar, Deauthentication of IP Drones and Cameras that Operate on 802.11 Wifi Standards using Esp8266, *International Journal of Electronics and Communication Engineering and Technology*, 10(2), 2019, pp. 23-30.
http://www.iaeme.com/IJECET/issues.asp?JType=IJECET&VType=10&IType=2

1. INTRODUCTION

The most recent couple of years have seen an emotional blast in the remote Innovation industry, henceforth, expanding the quantity of clients of wifi gadgets. Through some exploratory investigations, we trust that the ESP8266 Wi-Fi module is helpful for de-authenticate wifi. The ESP8266 Wi-Fi module is an independent System on-chip (SOC) with coordinated TCP/IP convention stacks that can give any microcontroller access to a Wi-Fi arrange. The ESP8266 is able to do either facilitating an application or offloading all Wi-Fi organizing capacities to another application processor.

The ESP8266 module is a board with a gigantic, and consistently developing, network of clients. This module has sufficiently incredible on-board preparing and capacity ability to enable it to be coordinated with the sensors and other application-explicit gadgets through its universally useful info/yields (GPIOs), with negligible advancement in advance and insignificant stacking amid runtime. Its high level of on-chip coordination takes into account negligible outer hardware.

The ESP8266 Wi-Fi module is considered for de-authenticating. Through trial thinks about, we trust that the ESP8266 Wi-Fi module is exceptionally valuable for de-authenticating. Be that as it may, this paper is to teach individuals on refreshing there wifi principles from 802.11 to 802.11w as a result of the de-authentication of customer to Wi-Fi utilizing ESP8266.

2. LITERATURE REVIEW

The ESP8266 Wi-Fi module is an independent System on-chip (SOC) with coordinated TCP/IP convention stacks that can give any microcontroller access to a Wi-Fi arrange. The ESP8266 module is a very financially savvy board with a colossal, and regularly developing, network of clients. This module has sufficiently amazing on-board preparing and capacity ability to enable it to be incorporated with the sensors and other application-explicit gadgets through its broadly useful information/yields (GPIOs), with negligible improvement in advance and insignificant stacking amid runtime.

Its high level of on-chip incorporation takes into consideration insignificant outside hardware. The front-end module is intended to possess insignificant PCB space.

Here, Firstly the executed code is dumped into ESP8266 than to choose the objective customer to disengage him from WiFi and to deauthenticate. Station mode is the default-working mode for the ESP8266 connector. This mode is utilized to interface the independent framework on-chip (SOC) ESP8266 to a remote system. The connector goes about as a passageway empowering other Wi-Fi connectors to interface with it; along these lines, the connector can be utilized to make one's own remote system. In Station mode, the ESP8266 Wi-Fi module gets the information from the neighborhood controller's MCU utilizing sequential communication. In this mode, the ESP8266 focuses on the particular client and deauthenticate him from the WiFi without his consent.

The ESP8266 Wi-Fi module is executed by coding, testing and deauthenticating the wifi. Through test examines, we trust that the ESP8266 Wi-Fi module is exceptionally helpful for deauthenticating the wifi.

This paper is to instruct individuals to refresh there wifi norms from 802.11 to 802.11w as a result of the likelihood of deauthentication of customer to Wi-Fi utilizing ESP8266.

3. ESP8266 WIFI MODULE

3.1. Wi-Fi organizing

Wi-Fi is an innovation for remote neighborhood with gadgets dependent on the IEEE 802.11 models.

Wi-Fi is a trademark of the Wi-Fi Collusion, which confines the utilization of the term Wi-Fi Confirmed to items that effectively total interoperability affirmation testing. Gadgets that can utilize Wi-Fi innovation incorporate PCs, computer game consoles etc., Wi-Fi good gadgets can associate with the Web by means of a WLAN organize and a remote access point. Such a passageway (or hotspot) has a scope of around 20 meters inside and a more noteworthy range outside.

Hotspot inclusion can be as little as a solitary stay with dividers that square radio waves, or as vast the same number of square kilometers accomplished by utilizing different covering passageways. Wi-Fi most normally utilizes the 2.4 gigahertz UHF and 5 gigahertz SHF ISM radio groups.

Having no physical associations, it is more defenseless against assault than wired associations, for example, Ethernet. Website pages that utilization Transport Layer Security (TLS) are secure, yet decoded Web access can without much of a stretch be distinguished by interlopers. For assurance, Wi-Fi has embraced different encryption advancements. The Wi-Fi Collusion has since refreshed its test plan and confirmation program to guarantee all recently affirmed gadgets oppose assaults. ESP8266 executes TCP/IP and full 802.11 b/g/n WLAN MAC convention. It underpins Basic Service Set (BSS) STA and Soft AP tasks under the Distributed Control Function (DCF). Power the board is taken care of with least host collaboration to limit dynamic obligation period.

3.2. ESP Wi-Fi module

The Center processor ESP8266 in littler sizes of the module epitomizes Tensilica L106 incorporates industry-driving ultra-low power 32-bit MCU miniaturized scale, with the 16-bit short mode, clock speed bolster 80 MHz, 160 MHz, underpins the RTOS, coordinated Wi-Fi Macintosh/BB/RF/Dad/LNA, on-board reception apparatus. The module bolsters standard IEEE802.11 b/g/n understanding, total TCP/IP convention stack. Users can utilize the add modules to a current gadget systems administration, or building a different system controller. ESP8266is high coordination remote SOCs, intended for space and power compelled versatile stage creators. It gives magnificent capacity to install Wi-Fi abilities inside different frameworks, or to work as an independent application, with the most reduced expense, and insignificant space necessity.

3.3. High Durability

ESP8266 is equipped for working reliably in modern situations, because of its wide working temperature go. With exceptionally incorporated on-chip highlights and negligible outer discrete part check, the chip offers unwavering quality, smallness and vigor.

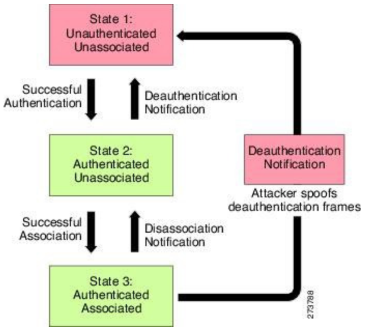
3.4. Compactness

ESP8266 is coordinated with a 32-bit Tensilica processor, standard advanced fringe interfaces, reception apparatus switches, RF balun, control enhancer, low clamor get intensifier, channels and power the board modules.

4. DEAUTHENTICATION

De-authentication acts exceptionally. The IEEE 802.11 (Wi-Fi) convention contains the arrangement for a de-authentication outline. Sending the casing from the passageway to a station is known as an "endorsed procedure to educate a rebel station that they have been separated from the system.

A de-authentication assault is just conceivable because of a weakness in the WiFi (802.11) standard. The deauther does not interfere with any frequencies, it is simply sending a couple of WiFi bundles that let certain gadgets detach. That empowers you to explicitly choose each objective.


State 1: Unauthenticated Unassociated
Successful Authentication
Deauthentication Notification
State 2: Authenticated Unassociated
Successful Association
Disassociation Notification
State 3: Authenticated Associated
Deauthentication Notification
Attacker spoofs deauthentication frames
273788

5. FEATURES OF ESP8266

The highlights of ESP Wi-Fi module are as per the Following:

- 802.11 b/g/n
- 802.11n support (2.4 GHz), up to 72.2 Mbps
- Defragmentation
- 2 x virtual Wi-Fi interface
- Automatic beacon monitoring (hardware TSF)
- Support Infrastructure BSS Station mode/Soft AP mode/Promiscuous mode
- Antenna diversity
- Coordinated low power 32-bit MCU
- Coordinated 10-bit ADC
- Coordinated TCP/IP convention stack
- Coordinated TR switch, balun, LNA, control intensifier and coordinating system
- Incorporated PLL, controllers, and power the board units
- Backings reception apparatus assorted variety
- Wi-Fi 2.4 GHz, support WPA/WPA2
- Bolster Shrewd Connection Capacity for both Android and iOS gadgets
- Profound rest control <10uA, Shut down spillage current < 5uA
- Wake up and transmit parcels in < 2ms
- Backup control utilization of < 1.0mW (DTIM3)
- +20dBm yield control in 802.11b mode
- Low-power, highly-integrated Wi-Fi solution
- A minimum of 7 external components
- Wide temperature range: -40°C to +125°C

5.1. IEEE 802.11

- IEEE 802.11 discharged in 1997
- Specifies two crude information rates of 1 and 2 (Mbit/s).
- It is infrared (IR) signals or by either Frequency bouncing or Direct-arrangement spread range in the Industrial Scientific Medical recurrence band at 2.4 GHz.
- IR remains a piece of the standard however has no real usage.

- The unique standard additionally characterizes Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the medium access technique.

5.1.1. 802.11 disadvantages

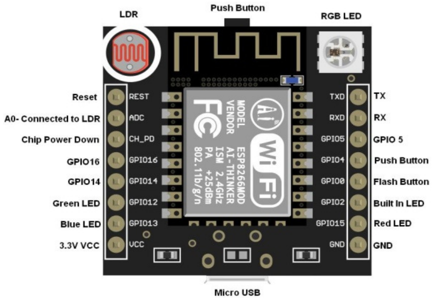
- It offered such huge numbers of decisions that interoperability was here and there testing to figure it out.
- It is actually to a greater degree a beta-determination than an inflexible particular, permitting singular item sellers the
- flexibility to separate their items.

5.2. IEEE 802.11w

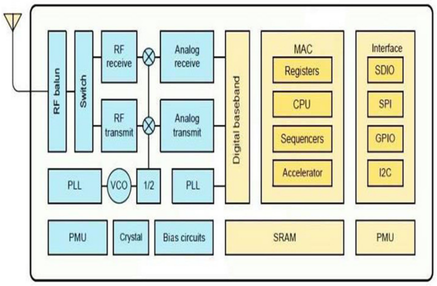
- IEEE 802.11w is the Protected Management Frames standard for the IEEE 802.11 group of principles.
- TGw is chipping away at improving the IEEE 802.11 Medium Access Control layer to expand the security of the board outlines.
- Wireless LANs send framework the executives data in unprotected edges, which makes them powerless.
- This standard will secure against system disturbance brought about by pernicious frameworks that produce disassociation asks for that seem, by all accounts, to be sent by legitimate hardware.
- It is normal that 802.11w would stretch out IEEE 802.11i to apply to 802.11 administration outlines just as information outlines.
- These augmentations will have communications with IEEE 802.11r and IEEE 802.11u

6. FIGURES

ESP8266 diagram:



Block diagram of ESP8266:



7. METHODOLOGY

The ESP8266 Wi-Fi module is an independent system on-chip (SOC) with incorporated TCP/IP convention stacks that can give any microcontroller access to a Wi-Fi arrange.

The wifi principles of 802.11 is defenseless and We can likewise play out an assortment of activities to test 802.11 remote systems by utilizing a cheap ESP8266 WiFi SoC (System on A Chip).

The fundamental element, the deauthentication assault, is utilized to separate gadgets from their WiFi arrange.

Nobody appears to think about this enormous powerlessness in the authority 802.11 WiFi standard so we took commencement to uncover its weakness and to prescribe the refreshed 802.11w WiFi measures.

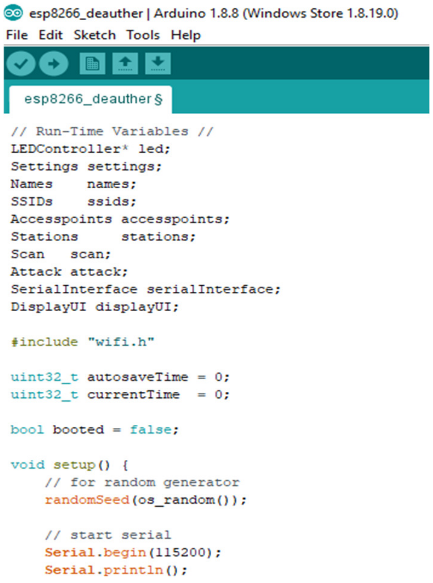
Here,Firstly the executed code is dumped into ESP8266 by utilizing Aurdino than to choose the objective with WiFi measures of 802.11 and after that to deauthenticate customer who is with the association with WiFi.

We trust it raises more consideration on the issue. Presently a days just a couple of organizations actualized it into their gadgets and programming.

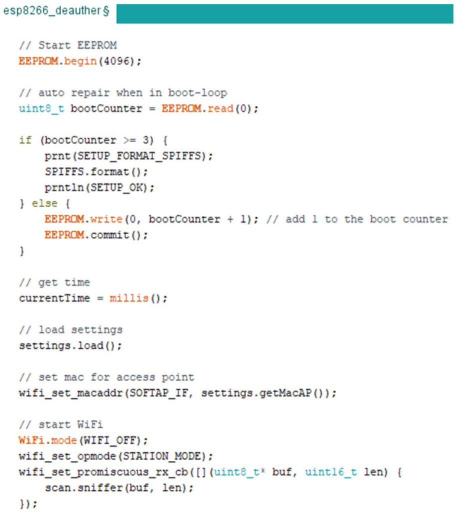
To viably keep a deauthentication assault, both customer and passage must help the 802.11w standard with secured administration outlines. While most customer gadgets appear to help it when the passageway compels it, essentially no WiFi passageway has it empowered.

Here we only take initiation to Expose the **immense defenselessness** of 802.11 Wi-Fi norm and Suggest the user to refresh their norm from 802.11 to 802.11w.

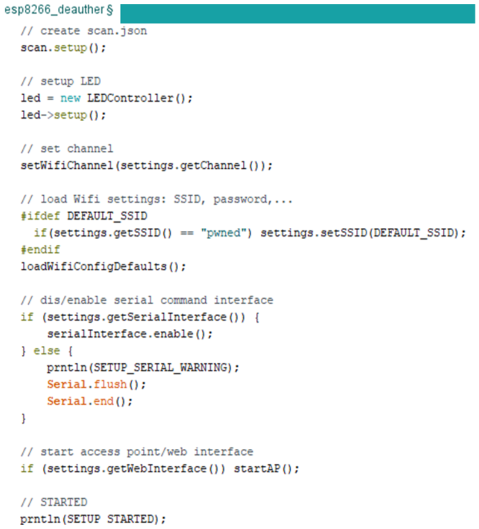
8. CODE


esp8266_deauther | Arduino 1.8.8 (Windows Store 1.8.19.0)
File Edit Sketch Tools Help
esp8266_deauther §

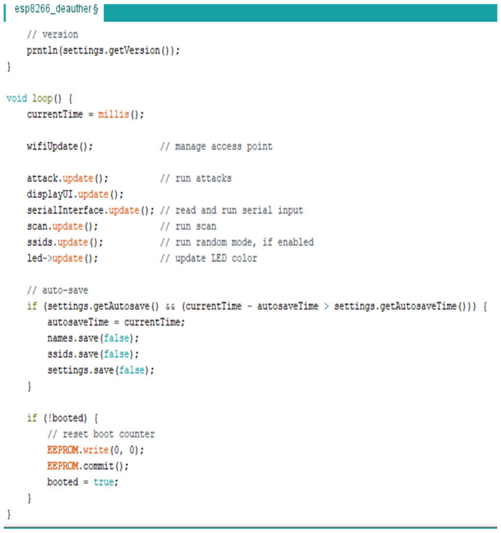
```
// Run-Time Variables //
LEDController* led;
Settings settings;
Names    names;
SSIDs    ssids;
Accesspoints accesspoints;
Stations     stations;
Scan   scan;
Attack attack;
SerialInterface serialInterface;
DisplayUI displayUI;

#include "wifi.h"

uint32_t autosaveTime = 0;
uint32_t currentTime  = 0;

bool booted = false;

void setup() {
    // for random generator
    randomSeed(os_random());

    // start serial
    Serial.begin(115200);
    Serial.println();
```



```
// Start EEPROM
EEPROM.begin(4096);

// auto repair when in boot-loop
uint8_t bootCounter = EEPROM.read(0);

if (bootCounter >= 3) {
    prnt(SETUP_FORMAT_SPIFFS);
    SPIFFS.format();
    prntln(SETUP_OK);
} else {
    EEPROM.write(0, bootCounter + 1); // add 1 to the boot counter
    EEPROM.commit();
}

// get time
currentTime = millis();

// load settings
settings.load();

// set mac for access point
wifi_set_macaddr(SOFTAP_IF, settings.getMacAP());

// start WiFi
WiFi.mode(WIFI_OFF);
wifi_set_opmode(STATION_MODE);
wifi_set_promiscuous_rx_cb([](uint8_t* buf, uint16_t len) {
    scan.sniffer(buf, len);
});
```



```
// create scan.json
scan.setup();

// setup LED
led = new LEDController();
led->setup();

// set channel
setWifiChannel(settings.getChannel());

// load Wifi settings: SSID, password,...
#ifdef DEFAULT_SSID
  if(settings.getSSID() == "pwned") settings.setSSID(DEFAULT_SSID);
#endif
loadWifiConfigDefaults();

// dis/enable serial command interface
if (settings.getSerialInterface()) {
    serialInterface.enable();
} else {
    prntln(SETUP_SERIAL_WARNING);
    Serial.flush();
    Serial.end();
}

// start access point/web interface
if (settings.getWebInterface()) startAP();

// STARTED
prntln(SETUP STARTED);
```



```
    // version
    prntln(settings.getVersion());
}

void loop() {
    currentTime = millis();

    wifiUpdate();              // manage access point

    attack.update();           // run attacks
    displayUI.update();
    serialInterface.update(); // read and run serial input
    scan.update();             // run scan
    ssids.update();            // run random mode, if enabled
    led->update();             // update LED color

    // auto-save
    if (settings.getAutosave() && (currentTime - autosaveTime > settings.getAutosaveTime())) {
        autosaveTime = currentTime;
        names.save(false);
        ssids.save(false);
        settings.save(false);
    }

    if (!booted) {
        // reset boot counter
        EEPROM.write(0, 0);
        EEPROM.commit();
        booted = true;
    }
}
```

9. CONCLUSIONS

By implementing the code and downloading it into the ESP8266 wifi module using Arduino, then we can select the targeted client and de-authenticate him from any WiFi, Drones (or) IP cameras which are using 802.11 wifi standards can be easily disconnected by using inexpensive wifi module like ESP8266 without the owner's permission.

We have successfully disconnected drones and IP cameras that operate on 802.11 Wifi standards. There is no other way to prevent this de-authentication we need to update our wifi standards to 802.11w.

As a responsible person while utilizing this device Capability be aware of the consequences before miss-using this device don't utilize it against others without their consent here we only take initiation to Expose the immense defenselessnes of 802.11 Wi-Fi norm and Suggest the user to refresh there norm from 802.11 to 802.11w!

REFERENCES

[1] http://www.esp8266.com/

[2] http://rancidbacon.com/files/kiwicon8/ESP8266_WiFi_Module_Quick_Start_Guide_v_1.0.4.pdf

[3] http://download.arduino.org/products/UNOWIFI/0A-ESP8266-Datasheet-EN-v4.3.pdf

[4] http://www.exptech.de/pdf/products/ESP07/Aithinker%20ESP07%20WIFI%20Module-EN.pdf

[5] https://www.engpaper.com/mobilejammer.html

[6] https://www.espressif.com/en/products/hardware/esp8266ex/overview

[7] https://www.espressif.com/sites/default/files/documentation/0aesp8266ex_datasheet_en.pdf

[8] https://www.academia.edu/31123117/esp8266_wifi_module_for_monitoring_system_application.