Smart Watch For Wi-Fi DE-Authentication In Restricted Area

Ms.J. Sriarunaa[1], Dharani Kumar. B[2], Jayachandran.R[3], John Yabaz.S[4], Suresh.S[5]
[1]Assistant professor, Dept of Electronics And Communication Engineering
[2, 3, 4, 5]Dept of Electronics And Communication Engineering
[1, 2, 3, 4, 5] Apollo Engineering College

Abstract- *In this project we are implementing smart watch for de-authenticating Wi-fi. With the help of this watch, we can be able to de-authenticate the Wi-fi connection in restricted areas. Here the microcontroller Node MCU (ESP8266) is used to de-authenticate the Wi-fi within the range of 45meters and the frequency 2.5GHz. The microcontroller is encoded with the type of DOS attack. This attack sends disassociate packet to one or more clients which are currently associated with access point. By sending the disassociated packets of DOS attack the Wi-fi user will not be able to use the Wi-fi within the range. The service provider signal will be disconnected manually by using the watch.*

Keywords- wi-fi modules, wi-fi, Dos Attack, De-authentications, Esp8266, secure restricted area.

I. INTRODUCTION

The ESP8266 Wi-Fi module is helpful for de-authenticate Wi-fi. 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 can do either facilitating an application or offloading all Wi-Fi organizing capacities to another application processor. This module has sufficiently incredible on-board preparing and capacity ability to enable it to be coordinated with the sensors with negligible advancement and insignificant stacking amid runtimes. By using advanced techniques of wi-fi modules we can able to perform de-authentication over the range of 2.5GHz.

ESP8266 WIFI MODULE

The Center processor ESP8266 in littler sizes of the module epitomizes Ten silica 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 conventional 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.

MAX30100

The MAX30100 is an integrated pulse oximetry and heart- rate monitor sensor solution. It combines two LEDs, a photodetector, optimized optics, and low-noise analog signal processing to detect pulse oximetry and heart-rate signals.

PULSE SENSOR

The Heartbeat rate information knowing is very useful while doing exercise, studying. But the heartbeat rate can be complicated to calculate. To overcome this problem, the pulse sensor or heartbeat sensor is used. This sensor mainly designed for Arduino board which can be used by makers, students, developers who can utilize the heartbeat information into their projects. This sensor uses an easy optical pulse sensor along with amplification & cancellation of noise to make a circuit. By using this circuit, we can get fast and reliable heartbeat readings. This circuit can be operated with 4mA current and 5V voltage to use in mobile applications.

18B20 TEMPERATURE SENSOR

Temperature sensors is an electronic device that used to measure the degree of temperature and convert the input data into electronic data to record or monitor temperature changes. The effective operating range is -50 to 250 degrees Celsius for glass encapsulated thermistors or 150 degrees Celsius for standard thermistor. When the voltage increases, the temperature also increases and vice versa.

ARDUINO UNO

Arduino is an open-source microcontroller-based electronic prototyping board that can be programmed using the easy-to-use Arduino IDE. Arduino consists of both a physical programmable circuit board and a software or IDE part. The Arduino IDE uses a simplified version of C++, making it easier to learn. The UNO is one of the most popular boards in the Arduino family. The Arduino board can be powered using an AC-to-DC adapter or a battery. The power supply can be connected by inserting the 2.1mm center positive plug into the board's power connector. The Arduino UNO board operates at 5 volts but can handle a maximum voltage of 20 volts. The Arduino UNO board has 6 analog input pins, labeled "analog 0-5". These pins can read a signal from an analog sensor, such as a temperature sensor, and convert it to a digital value to understand the system.

II. WORKING PRINCIPLE

Ade-authentication attack disrupts connections between users and Wi-Fi access points. The attackers force devices to lose access and then reconnect to a network they control. Then, perpetrators can track connections, capture login details, or trick users into installing rogue programs.

When the user switch on the wi-fi for checking the other wi-fi users for de-authenticate in the restricted areas. The screen will show the available wi-fi networks with that we can restrict the user for security purpose, and we can restrict multiple wi-fi networks. No other network can be in using that the moment. And we can measure the temperature, pulse, heartbeat of the watch user. After the completion we can remove or authenticate the wi-fi user around the restricted areas. There is no other way for authenticate the users.

III. BLOCK DIAGRAM

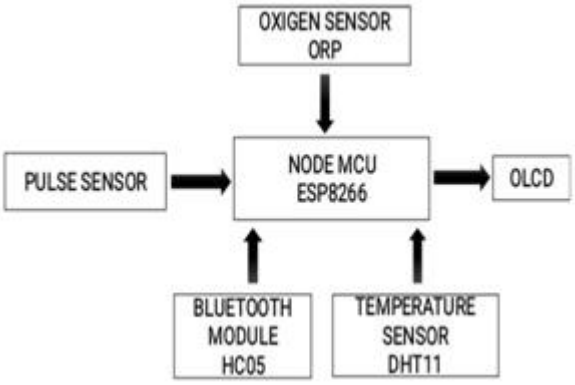

Fig no.1.1

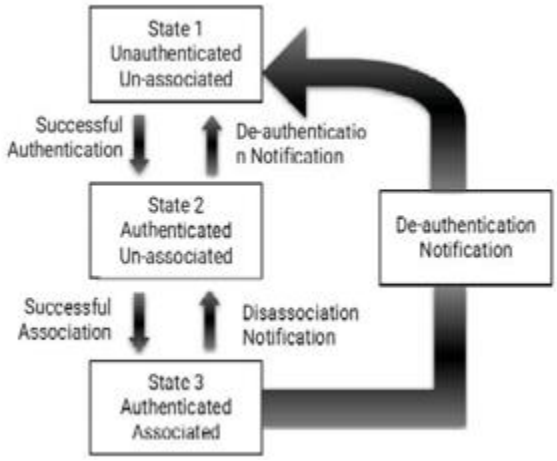

Fig no 1.2

IV. OUTPUT

The Temperature, Pulse, Heartbeat parameters are shown in the display and the de-authentication of wi-fi has been performed using the configurations in the diplay

Fig no 1.3

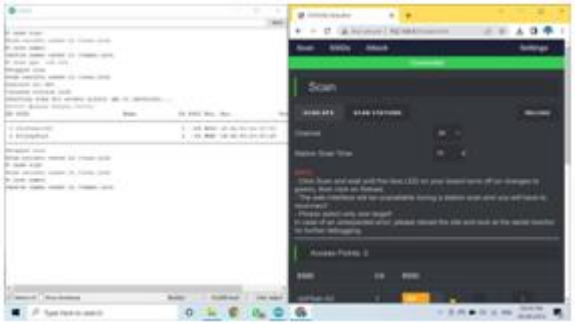

Fig no 1.4

The above fig no 1.3 shows the scanning process for checking the available Wi-Fi networks. When the scan button is pressed, and the web screen will show the wi-fi networks available around the particular area for the further steps.

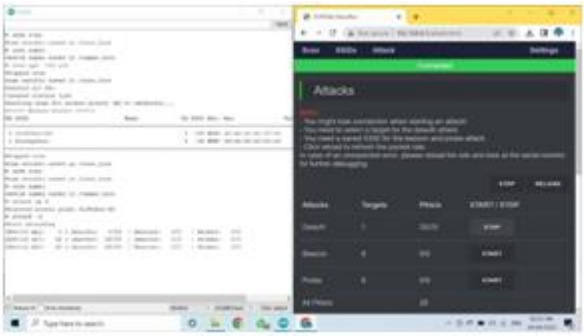

Fig no 1.5

The above fig no 1.5 shows the available wi-fi networks. Using the start button, we can de-authenticate the wi-fi. By pressing the start button the wi-fi network will get attacked and the wi-fi will disconnect.

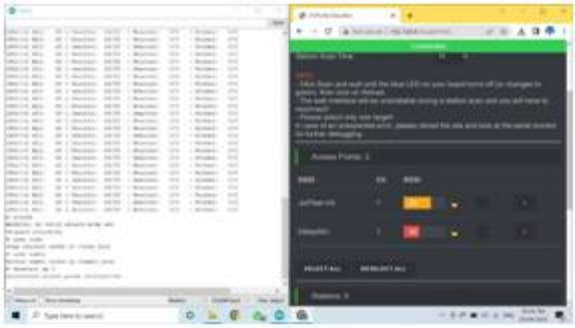

Fig no 1.6

This fig no 1.6 shows that the multiple number of wi-fi users can be de-authenticated at the same time by clicking on the select all option and attack.

V. CONCLUSION

By implementing the code and downloading it into the ESP8266 wi-fi module We have successfully disconnected drones and IP cameras that operate on 802.11 Wi-fi standards. There is no other way to prevent this de-authentication we need to update our wi-fi 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 defenselessness of 802.11 Wi-Fi norm and suggest the user to refresh their norm from 802.11 to 802.11w!. Memory and range of the microcontroller can be increased for the further compact size and design.

REFERENCES

[1] Thuc D. Nguyen, Duc H. M. Nguyen, Bao N. Tran, Hai VuNeeraj Mittal "A lightweight solution for defending against de-authentication/ disassociation attacks on 802.11 networks", IEEE, 2008.

[2] Domien Schepers, Aanjhan Ranganathan, Mathy Vanhoef, "On the Robustness of Wi-Fi De-authentication Countermeasures", San Antonio, 2022.

[3] Chintan Kamani, Dhrumil Bhojani, Ravi Bhagyoday, Vivek Parmar, Deepti Dave, "De-Authentication Attack on Wireless Network", International Journal of Engineering and Advanced Technology, 2019.

[4] Hadeel S. Obaid, "Denial of Service Attacks: Tools and Categories", International Journal of Engineering Research & Technology, 2020.

[5] Prof. Svapnil Vakharia, Bandi Vamsi Dharma Teja, "Overview of Wireless Network attacks and Security measures", IJRTI, 2017.

[6] Patrick LaRoche, A. Nur Zincir-Heywood, "802.11 De-authentication Attack Detection using Genetic Programming", IEEE, 2020.

[7] Richard Stehlik, "Wi-Fi attacks using ESP32", Excel fit, 2021.