SIGNAL PAUSER

A PROJECT REPORT

Submitted by

R. LOKESH	211801390031
P.S BHARATH KUMARACHARI	211801390022
E. PAVAN KUMAR	211801390015
P. SWETHA	211801390026
A.MANOJ	211801130008
P. AJAY	211801390001
K.SIMON SWAROOP	211801390023
T. SATHEESH	211801390020

Under the esteemed guidance of
Mr. Mangaldeep Chakraborty,
Teaching Associate

in partial fulfilment for the award of
the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE AND ENGINEERING

Centurion UNIVERSITY
Shaping Lives...
Empowering Communities...

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF ENGINEERING AND TECHNOLOGY
VIZIANAGARAM CAMPUS
CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT
ANDHRA PRADESH

DECEMBER 2023 / MAY 2024

BONAFIDE CERTIFICATE

Certified that this project report **SIGNAL PAUSER** is the bonafide work of "**R.LOKESH(211801390031),P.S.BHARATHKUMARACHARI(211801390022),E.PAVAN KUMAR(211801390015),P.SWETHA(211801390026),A.MANOJ(211801390008),P.AJAY(211801390001),K.SIMONSWAROOP(211801390023),T.SATHEESH(211801390020)"**who carried out the project work under my supervision. This is to further certify to the best of my knowledge, that this project has not been carried out earlier in this institute and the university.

SIGNATURE
MR. MANGALDEEP CHAKRABORTY
Teaching Assistant

Certified that the above mentioned project has been duly carried out as per the norms of the college and statutes of the university.

SIGNATURE
DR.P.SUBRAT KUMAR
HOD, ASSOCIATE PROFESSOR

HEAD OF THE DEPARTMENT / DEAN OF THE SCHOOL

Professor of Computer Science and Engineering
DEPARTMENT SEAL

DECLARATION

We hereby declare that the project entitled "**SIGNAL PAUSER**" submitted to the fulfilment of the award of the degree of B.Tech (Cse) in Centurion University of Technology and Management, Vizianagaram. This project work in original hasnot been submitted so far in any part or full for any other university or institute for the award of any degree or diploma.

R.LOKESH	211801390031
P. S BHARATH KUMAR ACHARI	211801390022
E. PAVAN KUMAR	211801390015
P. SWETHA	211801390026
P. AJAY	211801130001
P. MANOJ	211801390008
K. SIMON SWAROOP	211801390023
P. SATHEESH	211801390020

ACKNOWLEDGEMENT

We wish to express my profound and sincere gratitude to Mr. Mangaldeep Chakraborty Assistant Prof. Department of Computer Science and Engineering,SoET, Vizianagaram Campus, who guided me into the intricacies of this project nonchalantly with matchless magnanimity.

We thank Prof. Dr. Subrat Kumar Parida, Head of the Dept. of Department of Computer Science and Engineering, SoET, Vizianagaram Campus for extending their support during Course of this investigation.

We extend deep appreciation to Dr. P.A. Sunny Dayal, the Dean of SoET, for his help, leadership, and the conducive academic environment fostered at our institution. Their unwavering commitment to excellence has set a benchmark for all.

Special gratitude is extended to Dr. P.K. Mohanty, the Vice Chancellor of Centurion University, Vizianagaram, for providing a conducive and inspiring educational ecosystem.

A heartfelt note of appreciation goes to all staff members who, in various capacities, contributed to the success of our project. Dedication and collective efforthave been indispensable, and we sincerely thank them for their collaboration.

I express my deepest gratitude to my parents for their unwavering support, encouragement, and the countless sacrifices they made, which played an integral role in the success of this project.

ABSTRACT

This project focuses on developing a user-friendly interface for conducting denial-of- service (DoS) attacks on access points using readily available tools such as the ESP8266 and a data cable. The primary objective is to overload targeted access points with duplicate and extraneous data, rendering them temporarily inoperable anddisrupting connectivity for existing users. By creating an accessible interface, users withminimal technical expertise can select their desired target and execute the attack effortlessly. This initiative aims to shed light on the vulnerability of wireless networks and the ease with which individuals can exploit these weaknesses using simple hardware and tools Through the developed user interface, users can easily choose theirtarget access point and initiate the assault, leading to the flooding of the target with excessive data. Additionally, the use of a data cable enhances the attack's efficiency, allowing for a more controlled and directed approach. The project also highlights the ethical implications and the importance of raising awareness about the potential risksassociated with such attacks, emphasizing the need for improved security measures in wireless networks. Ultimately, this project serves as a demonstration of the susceptibility of commonly used access points to DoS attacks and the importance of reinforcing network security in the face of evolving threats.

INDEX

Table content:

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

The As the world becomes increasingly reliant on wireless networks for communication and connectivity, the security of these networks becomes paramount. However, with the proliferation of internet-connected devices and the rise of the Internet of Things (IoT), vulnerabilities in wireless infrastructure can be exploited with relative ease. This project delves into the realm of network security, focusing on the design and implementation of a user-friendly interface to conduct denial-of-service (DoS) attacks on access points. Leveraging the simplicity and accessibility of tools such as the ESP8266 microcontroller and a data cable, the project aims to highlight the potential risks associated with lax security measures in commonly used wireless networks. The objective of this undertaking is to draw attention to the vulnerability of access points, shedding light on the ease with which even individuals with limited technical expertise can disrupt wireless connectivity.

1.1 Purpose:

The purpose of the above project is to investigate and demonstrate the vulnerabilities present in wireless networks, specifically focusing on access points, by designing and implementing a user-friendly interface for conducting denial-of-service (DoS) attacks. The project aims to achieve several key objectives:

Raise Awareness: By showcasing how readily available tools like the ESP8266 and a data cable can be used to disrupt access points, the project aims to raise awareness about the potential risks associated with inadequate network security.

Highlight Vulnerabilities: Through the developed user interface, the project intends to highlight the vulnerabilities inherent in commonly used access points.

Encourage Ethical Considerations: The project serves as a platform to discuss the ethical implications of conducting such attacks and emphasizes the importance of responsible hacking practices.

Stimulate Security Discussions: The demonstration of a user-friendly interface for conducting DoS attacks aims to stimulate discussions about the evolving nature of cybersecurity threats.

1.2 Intended Audience:

The primary audience for this document includes:

Security Professionals and Researchers:

Security experts, researchers, and professionals in the field of cybersecurity who seek to understand and address vulnerabilities in wireless networks.

Educational Institutions:

Students and educators in computer science, information security, and related disciplines who can use the project as a practical example for learning about network vulnerabilities and ethical hacking.

Technology Enthusiasts:

Individuals with a general interest in technology and cybersecurity who want to gain a better understanding of the vulnerabilities in wireless networks and the ease with which certain attacks can be executed.

Security Awareness Programs:

Organizations conducting security awareness programs to educate employees about the potential risks associated with wireless networks and the importance of adhering to security best practices.

General Public:

The project may also serve as an eye-opener for the general public, fostering awareness about the vulnerabilities in everyday technologies and the need for responsible use of wireless networks.

1.3 Scope:

We want to make this device user-friendly to use. And make the security tests of the wi-fi networks in an easy and simple way. This user-friendly interface allows the users to perform security tests on the selected access-point's . The aforementioned project lies in its potential evolution into a robust and versatile tool for advancing network security practices. First and foremost, future developments could focus on the refinement of the user interface and functionality, aiming for a seamless and intuitive experience for users from diverse backgrounds. Enhancements could include the incorporation of machine learning algorithms to dynamically adapt to evolving attack patterns, providing a more adaptive and resilient defense against denial-of-service attacks. Additionally, the project could expand its capabilities to simulate a wider range of security threats, offering organizations a comprehensive platform to test and fortify their networks against various cyber threats beyond traditional denial-of-service scenarios.

CHAPTER 2: LITERATURE SURVEY

Literature Survey for Denial-of-Service Attacks on Wireless Networks Using ESP8266 and User-Friendly Interface

Wireless Network Security:

Investigate foundational literature on wireless network security, covering common vulnerabilities and attack vectors. Explore studies detailing the consequences of security breaches on wireless networks, emphasizing the importance of robust security measures.

Denial-of-Service Attacks:

Review academic papers and research articles on denial-of-service attacks, focusing on methodologies, tools, and countermeasures. Analyze case studies illustrating the impact of such attacks on network performance and user experience.

Microcontroller-Based Attacks:

Explore literature on microcontrollers, with a specific focus on the ESP8266. Investigate how microcontrollers are utilized in ethical hacking scenarios and their applications in wireless communication security.

User Interface for Hacking Tools:

Examine research that discusses the development of user interfaces for ethical hacking tools. Evaluate the impact of user-friendly interfaces on the accessibility and adoption of such tools by individuals with varying levels of technical expertise.

Ethical Hacking and Responsible Disclosure:

Investigate literature on ethical hacking practices, including guidelines for responsible disclosure. Understand the ethical considerations associated with using hacking tools for educational purposes and research, ensuring alignment with ethical standards.

Wireless Network Security Best Practices:

Review industry best practices and standards for securing wireless networks, with a specific emphasis on access point security. Identify studies that assess the efficacy of current security measures in preventing or mitigating denial-of-service attacks.

Collaborative and Open-Source Security Initiatives:

Explore literature on collaborative efforts within the ethical hacking community, open-source security tools, and frameworks. Investigate how collaborative projects contribute to advancing cybersecurity practices, knowledge-sharing, and the development of effective security solutions.

Simulation and Testing Environments:

Investigate literature related to simulation environments for testing security measures. Explore how organizations can safely simulate denial-of-service attacks to assess and improve their network defenses.

Regulatory Compliance and Standards:

Explore literature on regulatory compliance and industry standards related to wireless network security. Understand the evolving landscape of regulations and standards that impact network security practices.

Wireless Network Threat Landscape:

Examine research that provides insights into the evolving threat landscape of wireless networks. Identify emerging threats and vulnerabilities, and understand how the project can adapt to address new challenges.

CHAPTER 3: OVERALL DESCRIPTION

This project aims to explore and demonstrate the vulnerabilities present in wireless networks, specifically focusing on access points, through the implementation of a simulated denial-of-service (DoS) attack. The project utilizes the ESP8266 microcontroller, a versatile and widely available component, as the key tool for executing the simulated attacks. At the core of this endeavor is the development of a user-friendly interface, enabling individuals with varying technical backgrounds to easily select target access points and initiate the simulated DoS attacks. Grounded in a comprehensive literature survey encompassing wireless network security, ethical hacking practices, and microcontroller-based attacks, the project seeks to raise awareness about network vulnerabilities and educate users on responsible hacking practices.The project's objectives include fostering user accessibility by prioritizing an intuitive interface design, emphasizing ethical considerations, and promoting collaborative efforts within the ethical hacking community. Additionally, it aims to contribute to open-source security initiatives, align with industry standards, and facilitate a deeper understanding of network security challenges.

3.1 Existing System

Currently, the landscape of existing systems in the realm of denial-of-service (DoS) attack simulations on wireless networks is varied. Traditional tools used for ethical hacking and penetration testing may lack a user-friendly interface, making them less accessible to individuals with limited technical expertise. Moreover, while there are numerous open-source tools for simulating DoS attacks, they may not specifically target the ESP8266 microcontroller or provide a cohesive and intuitive user interface tailored for the purpose of conducting simulated attacks on access points.

3.1.1 Proposed System

The key components of the proposed system are outlined below:

User-Friendly Interface:

The heart of the proposed system is a user-friendly interface that simplifies the process of selecting target access points and initiating simulated DoS attacks.

ESP8266 Microcontroller Integration:

The system leverages the ESP8266 microcontroller, a widely used and versatile component in the realm of wireless communication. The integration of the ESP8266 ensures that the simulated attacks are tailored to address the vulnerabilities specific to this microcontroller and its applications.

Educational Emphasis:

The proposed system places a strong emphasis on education and awareness. It is designed to be a learning tool, allowing users to understand the intricacies of wireless network vulnerabilities and the potential impact of DoS attacks.

Ethical Considerations:

Ethical considerations are integral to the proposed system. It incorporates guidelines for responsible disclosure, promoting ethical hacking practices and ensuring that users are aware of the legal and ethical implications associated with the use of such tools.

Collaboration and Open Source:

The system is envisioned as a collaborative project, encouraging contributions from the ethical hacking community. It may be developed as an open-source tool, allowing for continuous improvement, community-driven enhancements, and the incorporation of industry best practices.

The main challenges in developing the proposed system lie in the intricacies of creating a user-friendly interface for initiating denial-of-service attacks on wireless networks. Designing a seamless and intuitive interface that caters to users with varying levels of technical expertise while maintaining the educational aspectof the tool is a significant usability challenge. Additionally, addressing the specific vulnerabilities associated with the ESP8266 microcontroller presents a technical hurdle, requiring in-depth knowledge and rigorous testing to ensure the simulated attacks effectively target wireless access points.

3.1.2 Operational Environment

Network Infrastructure:

The project operates within diverse network environments, encompassing various access points and configurations

ESP8266 Microcontroller Integration:

The operational environment involves the integration of the ESP8266 microcontroller into the wireless network.

User Interface Platform:

The user-friendly interface is designed to operate seamlessly on multiple platforms, ensuring accessibility for users across different devices, including desktop computers, laptops, and potentially mobile devices.

3.1.3 User Characteristics:

Students and Educators:

Academic institutions, students, and educators form a significant user group. The project is tailored to serve as an educational tool, providing a hands-on experience for understanding the vulnerabilities of wireless networks and the implications of denial-of-service attacks.

Ethical Hackers and Security Enthusiasts:

Individuals with a keen interest in ethical hacking, penetration testing, and network security represent another user category. The project offers a platform for exploration and experimentation, enabling users to simulate DoS attacks on access points and deepen their understanding of security practices.

3.1.4 System Requirements Specification

The successful deployment and operation of the proposed project, which involves simulating denial-of-service attacks on wireless networks using the ESP8266 microcontroller with a user-friendly interface, necessitate specific system requirements. These requirements encompass both hardware and software components:

Hardware Requirements:

ESP8266 Microcontroller:

The ESP8266 microcontroller, a central component of the project, is required for executing simulated denial-of-service attacks on wireless access points. The hardware should support the necessary programming interfaces and connectivity features.

Data Cable:

Data cable allows to communication between hardware components within a computer.

3.1.5 Functional Requirements:

User Authentication:

The system should incorporate user authentication mechanisms to control access and ensure that only authorized users can interact with the tool.

Target Selection:

Users should be able to select target wireless access points for simulated denial-of-service attacks through the user-friendly interface.

Attack Configuration:

The system should provide options for users to configure parameters of the simulated denial-of-service attacks, such as attack intensity, duration, and attack type.

ESP8266 Integration:

Integration with the ESP8266 microcontroller, allowing the tool to execute the simulated denial-of-service attacks on the selected wireless access points.

User-Friendly Interface:

Description: A graphical user interface (GUI) that is intuitive and user-friendly, facilitating easy navigation and interaction with the tool.

3.1.6 Non-Functional Requirements:

Performance:

The system should exhibit efficient performance, ensuring minimal latency during the execution of simulated denial-of-service attacks and providing timely feedback to users.

Scalability:

The system must be scalable to accommodate a varying number of users and adapt to different network environments, ensuring consistent performance under different loads.

Reliability:

The system should be reliable, with a low probability of failures or crashes during the execution of simulated attacks, to provide a stable and dependable user experience.

Usability:

Description: The user interface should be designed for high usability, ensuring ease of navigation and understanding for users with diverse technical backgrounds.

Security:

The system must implement robust security measures to prevent unauthorized access, protect user data, and mitigate potential risks associated with simulated attacks.

3.2 UML Diagrams:

UML is a method for describing the system architecture in detail using the blueprint. UML represents a collection of best engineering practices that have proven successful in the modelling of large and complex systems. UML is a very important part of developing objects-oriented software and the software development process. UML uses mostly graphicalnotations to express the design of software projects. Using the UML helps project teams communicate, and validate the architectural deof the software.

Definition: UML is a general-purpose visual modelling language that is used to specify, visualize,construct, and document the artifacts of the software system.

UML is a Language: It will provide vocabulary and rules for communications and function on conceptual and physical representation. So, it is modelling language.

UML Specifying: Specifying means building models that are precise, unambiguous and complete.In particular, the UML address the specification of all the important analysis, design and implementation decisions that must be made in developing and displaying a software intensive system.

UML Visualization: The UML includes both graphical and textual representation. It makes easyto visualize the system and for better understanding.

3.2.1 Usecase Diagram

The Figure 3.2.1 shows the use case diagram illustrates the various interactions and relationshipsbetween system and user in Tree Enumeration.

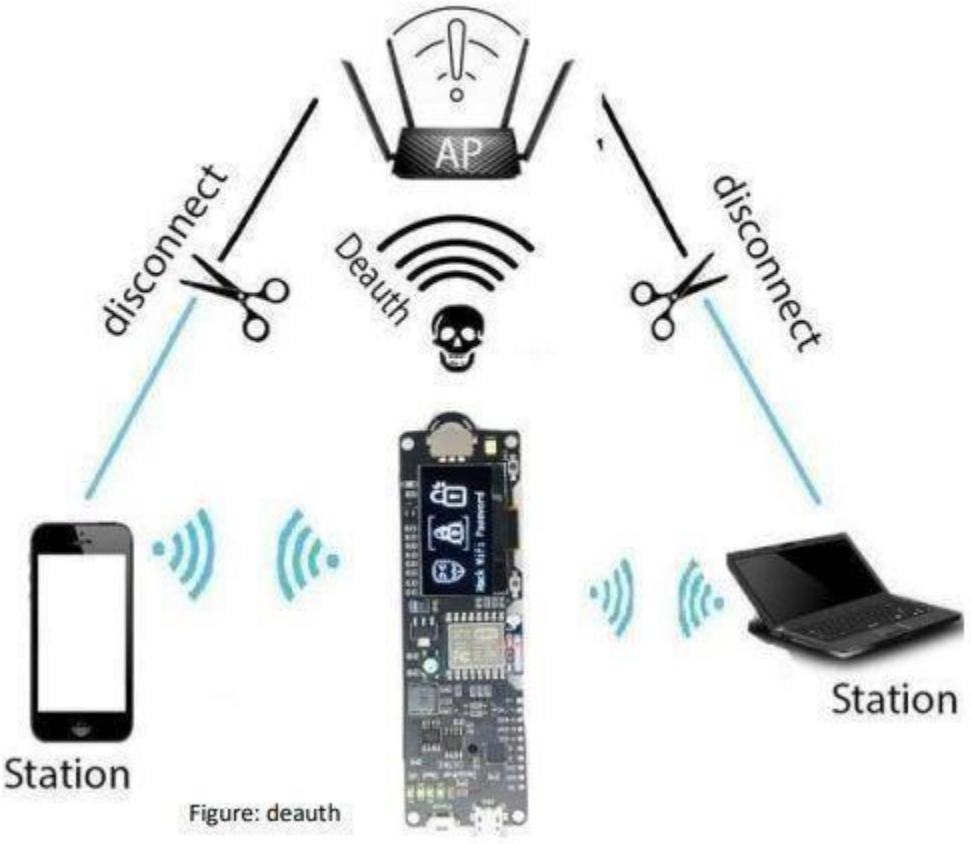


Figure 3.1: Use Case Diagram

3.2.2 Sequential Diagram:

The Figure 3.2.2 shows the sequence diagram shows the sequential order of interactions betweensystem components during specific use cases..

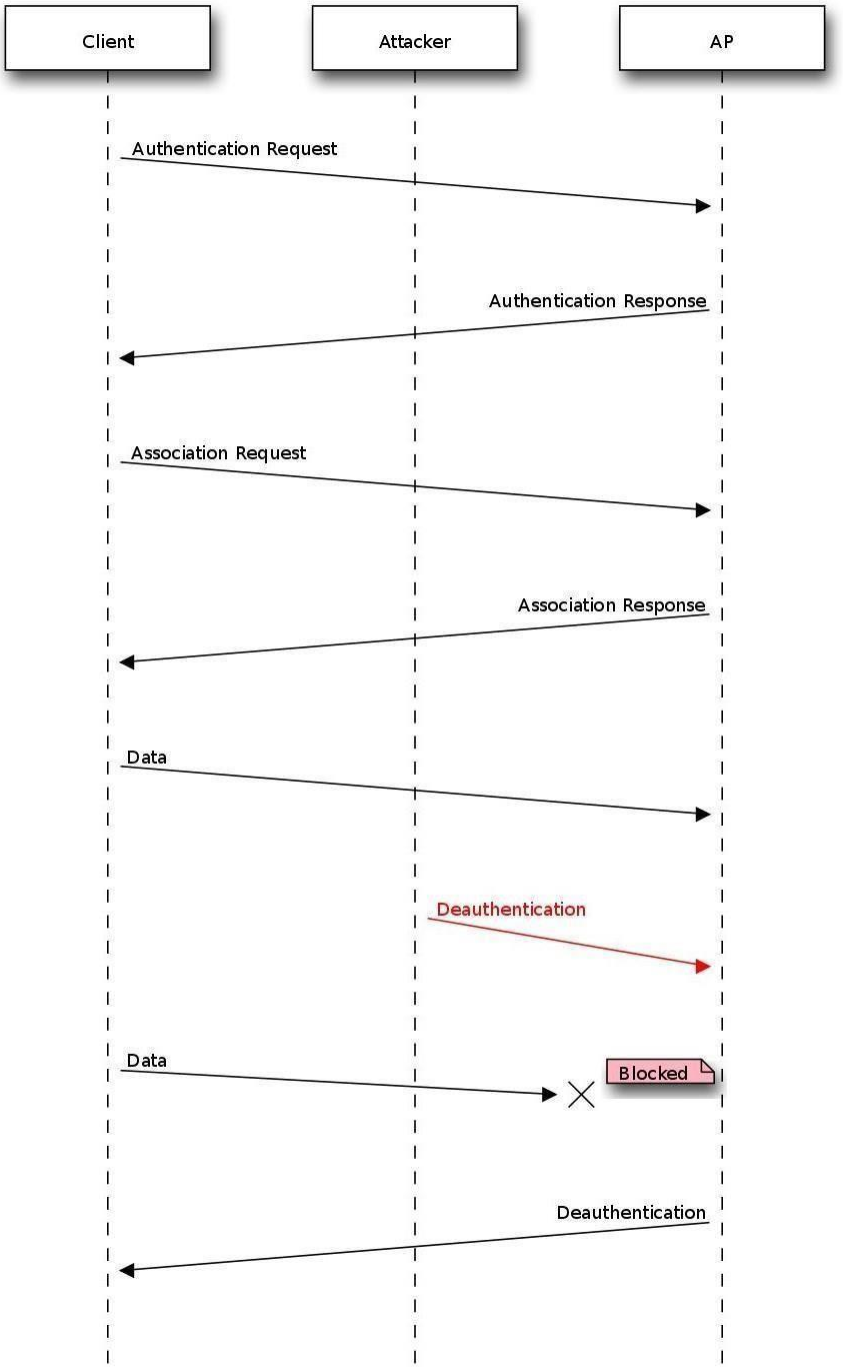


Figure 3.2: Sequential Diagram

3.2.3 Flow Chart

The proposed project's operational flow begins with user authentication, verifying that the user is authorized to engage with the simulation tool. Once authenticated, users proceed to select target wireless access points within the user-friendly interface. Subsequently, users configure parameters for the simulated denial-of-service attacks, including intensity, duration, and attack type. The system then integrates with the ESP8266 microcontroller to execute these simulated attacks on the chosen access points. Concurrently, real-time monitoring allows users to observe the impact on target access points and network performance. To ensure responsible usage, the system conducts a check against ethical guidelines and practices. Users are provided access to comprehensive documentation and educational resources, facilitating a deeper understanding of the tool's functionalities and ethical considerations. For those in collaborative environments, the system supports contribution through version control systems and online repositories. The operational flow concludes with the successful completion of the simulation, marked by the "End"point in the flowchart.

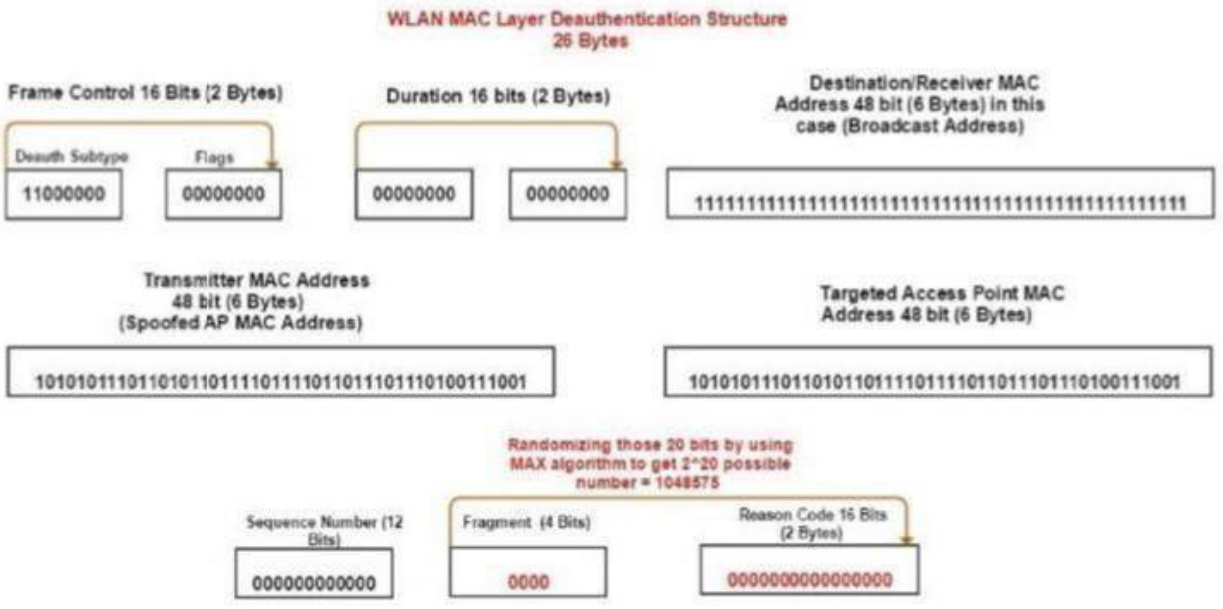
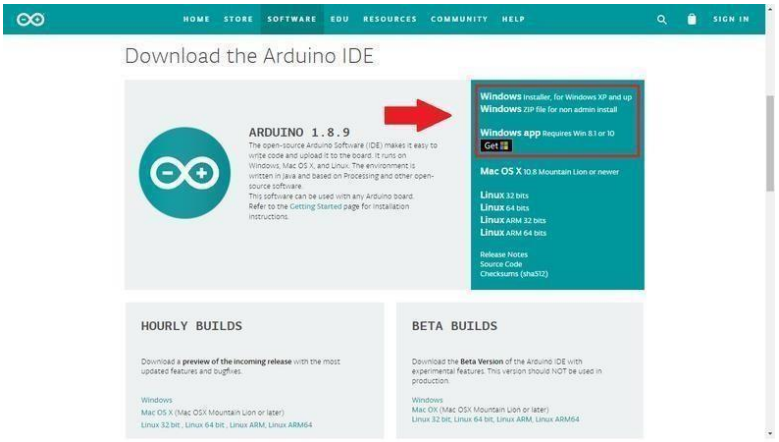


Figure 3.3: Flow chart diagram

Chapter 4: ARDUINO IDE

Step 1: Download File Arduino IDE



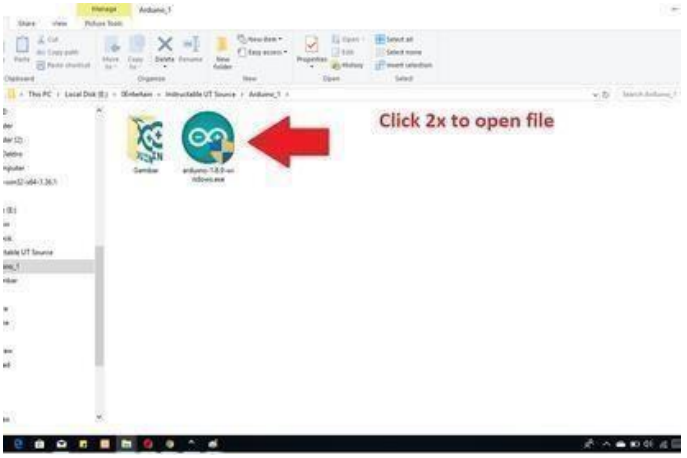


Fig:4.1

Click the link below to download the Software :

Arduino IDE Software

On that page, there are 3 download options for Windows.

- **Windows Installer** : The software will be installed in Windows operating system and required admin access.
- **Windows Zip file** : To make a portable installation.
- **Windows App** : for Windows 8.1 or 10.

I suggest the first option. because it directly install all your needs to use the Arduino IDE Software, and include **drivers** for the the Arduino board. If you choose the Zip file you need to install the driver manually.

Click Windows Installer, then click "*just download*" or "*Contribute & Download*".

After the download is complete, open the installer file and start installing.

Step 2: License Agreement

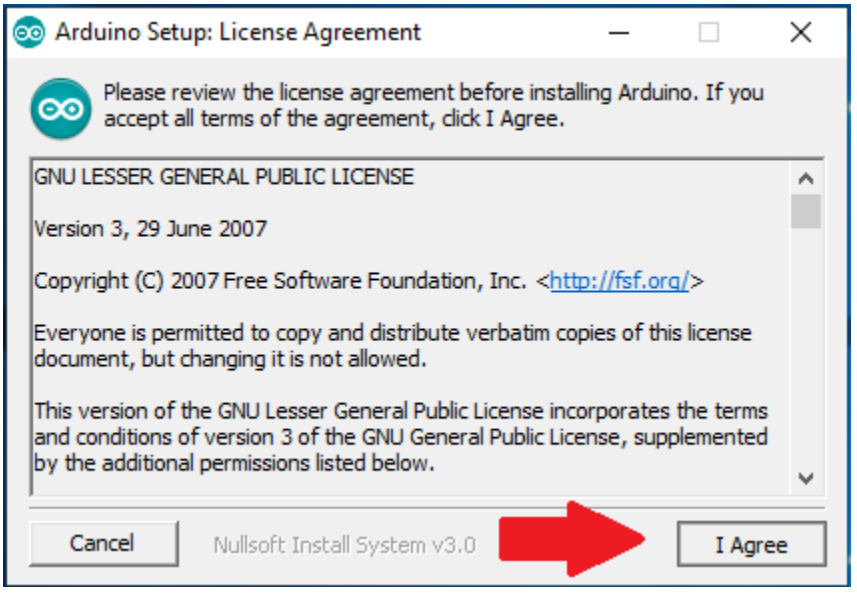


Fig:4.2

After the file is run, the “License Agreement” page will apper. You can read it, then click “*I Agree*” to continue.

Step 3: Installation Option

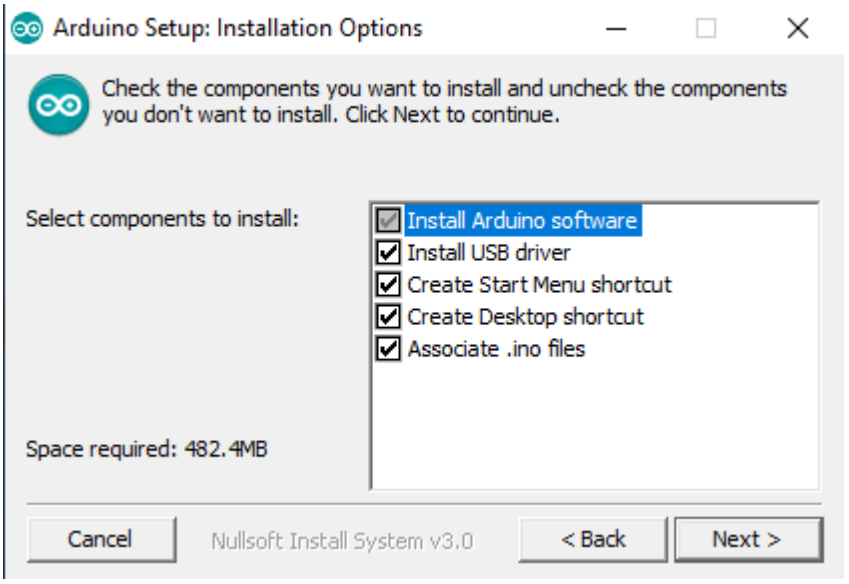


Fig 4.3

Check the component that you want to install and uncheck the components that you don't want to install. I suggest installing all components. Click "*next*" to continue.

Step 4: Installation Folder

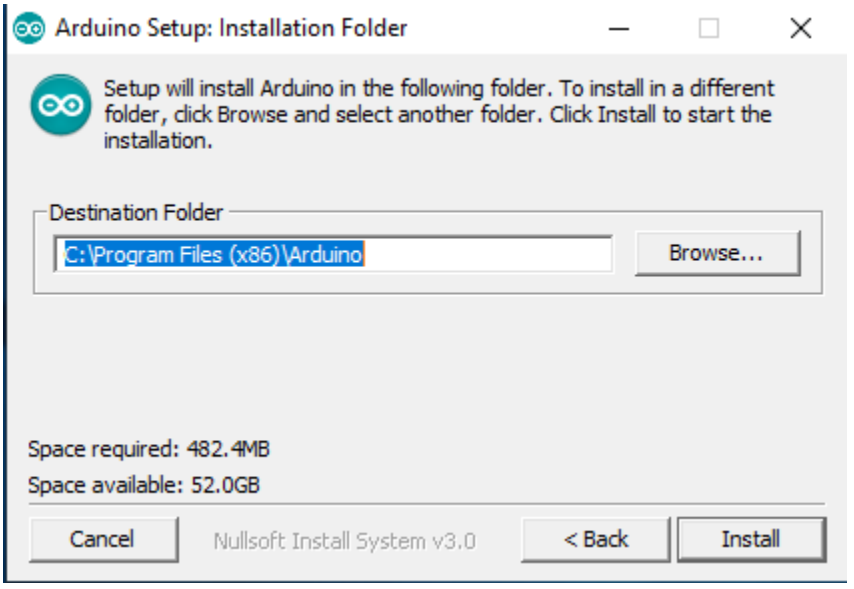


Fig.4.4

Arduino will automatically be installed in "**C:\Program Files (x86)\Arduino**". If you want to change the folder, click "*Browse*" and select the desired folder. Click install to start the installation.

Step 5: Installing Process

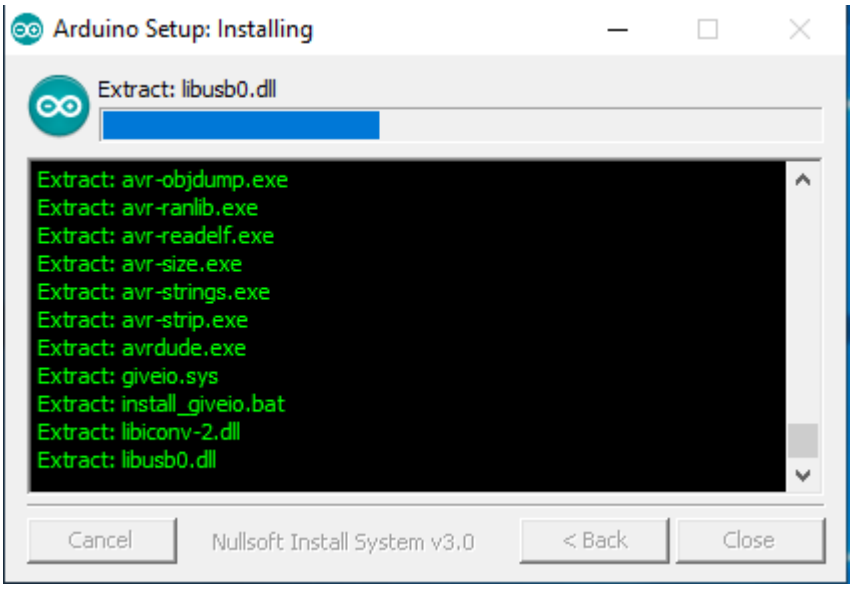


Fig.4.5

The installation process is ongoing.

Step 6: Installation Complete

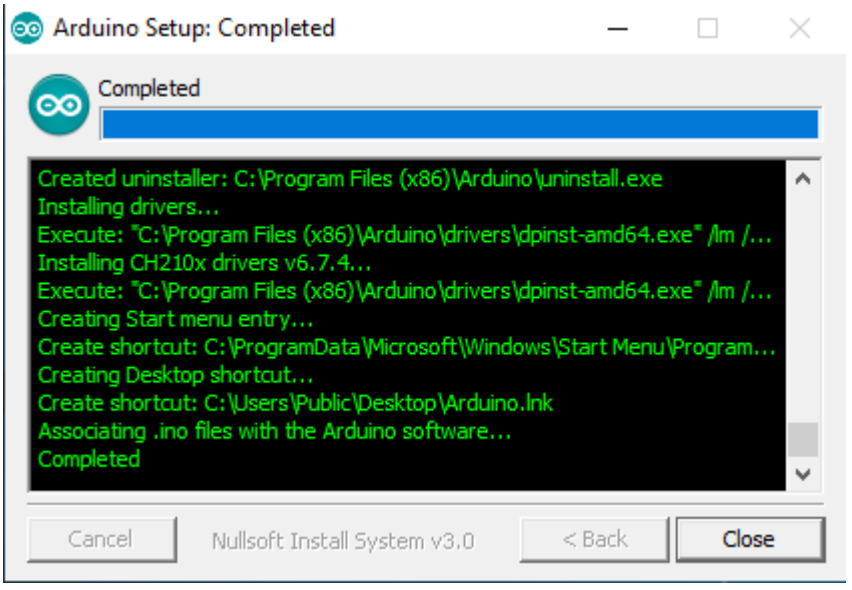


Fig.4.6

If there is written "*complete*", it means that the installation process is complete. click "*Close*".

Step 7: Open Arduino IDE

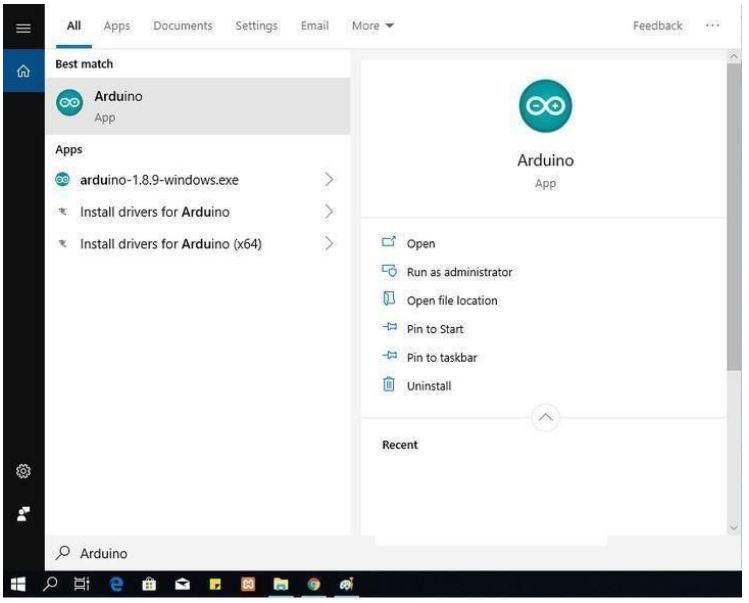


Fig.4.7

After the installation process is complete, there will be an Arduino icon on the Desktop. Or check on the search icon and write "23rduino". If you have found the 23rduino icon, run the application.

Step 8: Display Arduino IDE

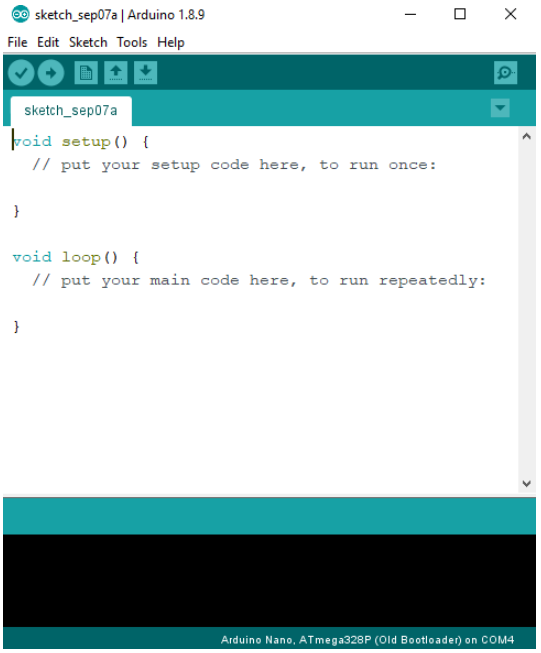


Fig.4.8

This is a display of the Arduino IDE Software. The application is ready to be used to create amazing projects. Wait for my next article about a simple project using Arduin

CHAPTER 5: IMPLEMENTATION

PROCEDURE

1. **Gather Components:**
   Ensure we have all the necessary components.
2. **Connect the ESP8266:**

   Connect the ESP8266 to cable.

3. **Write the Code:**
   Use the Arduino IDE with the ESP8266 board support or platforms like Platform IO for ESP8266 development.
4. **Upload/Run the Code:**
   Upload the code to the ESP8266 development board using the Arduino IDE or other suitable software. Make sure to select the correct board and port in the IDE before uploading.

6. Display or Output:

You can use the serial monitor for disconnect and connect the access-point.

7. Maintenance:

Regularly check and maintain the system to ensure proper functioning. Calibrate if necessary and replace components that wear out

Main code:

```
/* =====================

  This software is licensed under the MIT License:

  https://github.com/spacehuhntech/esp8266_deauther

  ====================  */

extern "C" {

   // Please follow this tutorial:

   //      https://github.com/spacehuhn/esp8266_deauther/wiki/Installation#compiling-using-arduino-ide

   // And be sure to have the right board selected

 #include "user_interface.h"

}

#include "EEPROMHelper.h"

#include "src/ArduinoJson-v5.13.5/ArduinoJson.h"

#include "oui.h"

#include "language.h"

#include "functions.h"

#include "settings.h"

#include "Names.h"
```

```
#include "SSIDs.h"
#include "Scan.h"
#include "Attack.h"
#include "CLI.h"
#include "DisplayUI.h"
#include "A_config.h"
#include "led.h"
#include "wifi.h"
// Run-Time Variables
Names names;
SSIDs ssids;
Accesspoints accesspoints;
Stations stations;
Scan scan;
Attack attack;
CLI cli;
DisplayUI displayUI;
simplebutton::Button* resetButton;
uint32_t autosaveTime = 0;
uint32_t currentTime = 0;
bool booted = false;
void setup() {
  // Initialize random generator
  randomSeed(os_random());
  // Start serial communication
  Serial.begin(115200);
  Serial.println();
  // Start SPIFFS
  prnt(SETUP_MOUNT_SPIFFS);
  LittleFS.begin();
  prntln(/*spiffsError ? SETUP_ERROR : */ SETUP_OK);
  // Start EEPROM
  EEPROMHelper::begin(EEPROM_SIZE);
  // Format SPIFFS when in boot-loop
  if    (!EEPROMHelper::checkBootNum(BOOT_COUNTER_ADDR))    {
```

```
    prnt(SETUP_FORMAT_SPIFFS);
    LittleFS.format();
    prntln(SETUP_OK);
    prnt(SETUP_FORMAT_EEPROM);
    EEPROMHelper::format(EEPROM_SIZE);
    prntln(SETUP_OK);
    EEPROMHelper::resetBootNum(BOOT_COUNTER_ADDR);
}
// Get time
currentTime = millis();
// Load settings
#ifndef RESET_SETTINGS
settings::load();
#else
settings::reset();
settings::save();
#endif
// Initialize WiFi
wifi::begin();
wifi_set_promiscuous_rx_cb([](uint8_t* buf, uint16_t len) {
    scan.sniffer(buf, len);
});
// Start display
if (settings::getDisplaySettings().enabled) {
    displayUI.setup();
    displayUI.mode = DISPLAY_MODE::INTRO;
}
// Load additional data
names.load();
ssids.load();
cli.load();
// Create scan.json
scan.setup();
// Enable/disable serial command interface
if (settings::getCLISettings().enabled) {
```

```
        cli.enable();
    } else {
        prntln(SETUP_SERIAL_WARNING);
        Serial.flush();
        Serial.end();
    }
    // Start access point/web interface
    if (settings::getWebSettings().enabled) wifi::startAP();
    // Initialization completed
    prntln(SETUP_STARTED);
    prntln(DEAUTHER_VERSION);
    // Setup LED
    led::setup();
    // Setup reset button
    resetButton = new ButtonPullup(RESET_BUTTON);
}
void  loop() {
    currentTime = millis();
    led::update(); // Update LED color
    wifi::update(); // Manage access point
    attack.update(); // Run attacks
    displayUI.update();
    cli.update(); // Read and run serial input
    scan.update();  // Run scan
    ssids.update();  // Run random mode if enabled
    // Auto-save
    if (settings::getAutosaveSettings().enabled &&
        (currentTime - autosaveTime > settings::getAutosaveSettings().time)) {
        autosaveTime = currentTime;
        names.save(false);
        ssids.save(false);
        settings::save(false);
    }
    // Boot flag handling
    if (!booted) {
```

```
        booted = true;
        EEPROMHelper::resetBootNum(BOOT_COUNTER_ADDR);
#ifdef HIGHLIGHT_LED
        displayUI.setupLED();
#endif
    }
    // Reset button handling
    resetButton->update();
    if (resetButton->holding(5000)) {
        led::setMode(LED_MODE::SCAN);
        DISPLAY_MODE _mode = displayUI.mode;
        displayUI.mode = DISPLAY_MODE::RESETTING;
        displayUI.update(true);
        settings::reset();
        settings::save(true);
        delay(2000);
        led::setMode(LED_MODE::IDLE);
        displayUI.mode = _mode;
    }
}
```

CHAPTER 6: OUTPUTS

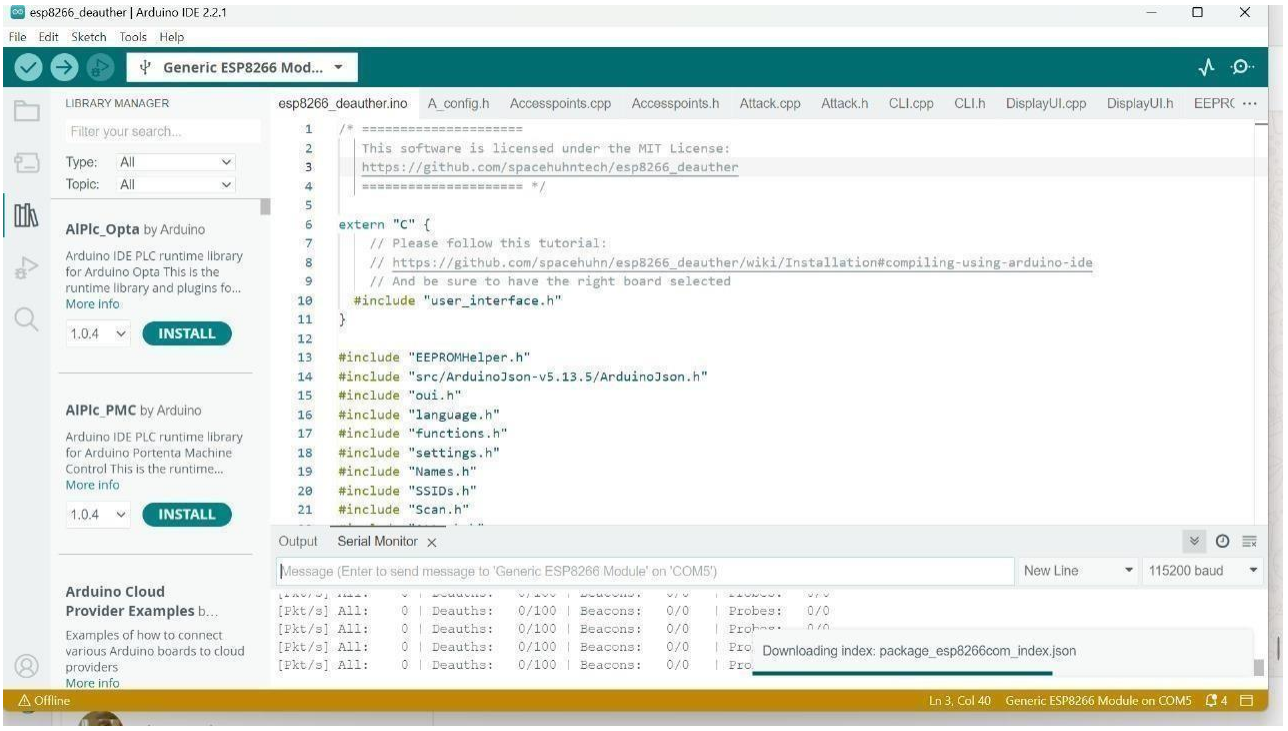
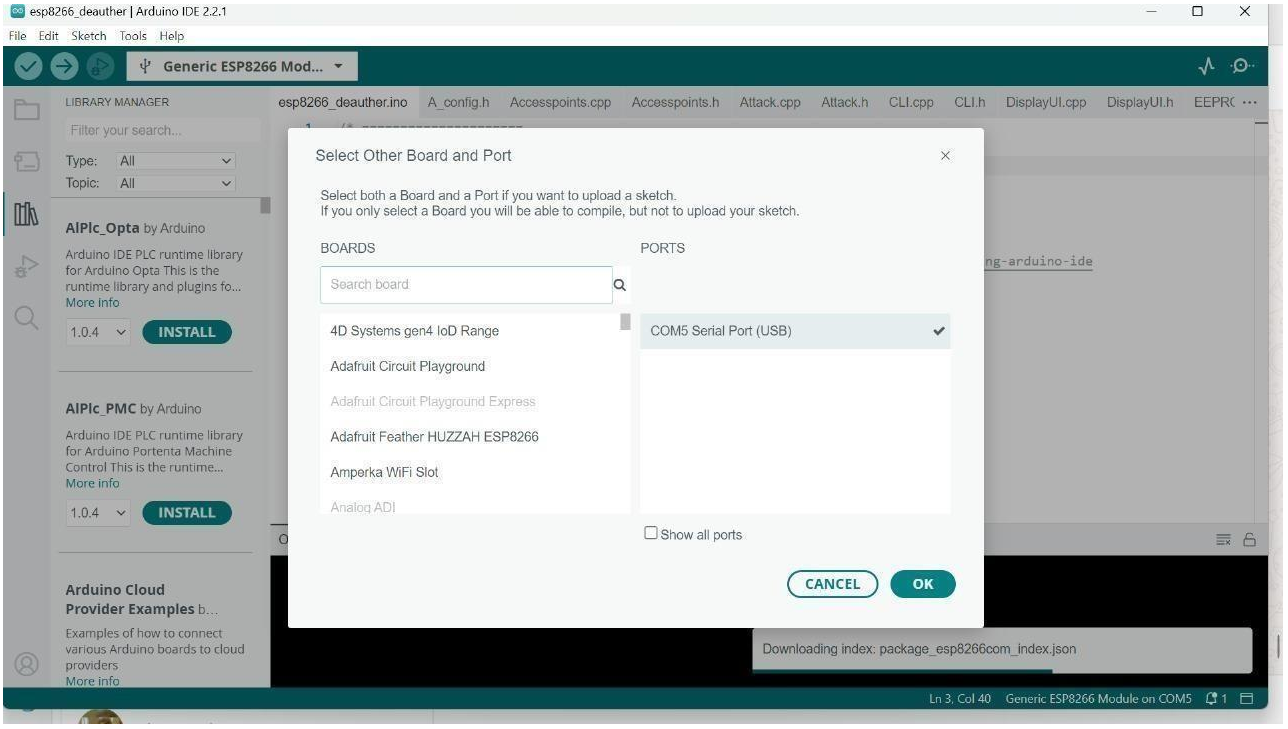
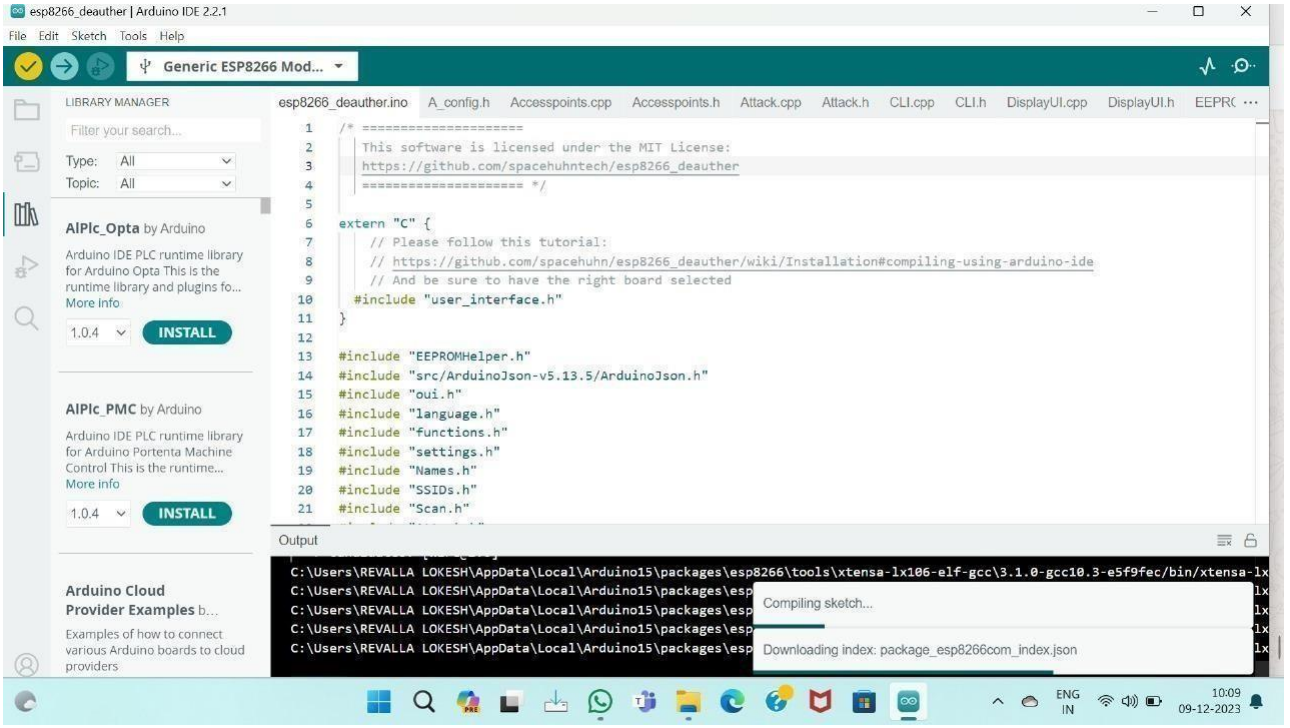


Fig.6.1 upload the code to IDE



Fig;6.2 selecting board and port



Fig;6.3 compileing the sketch

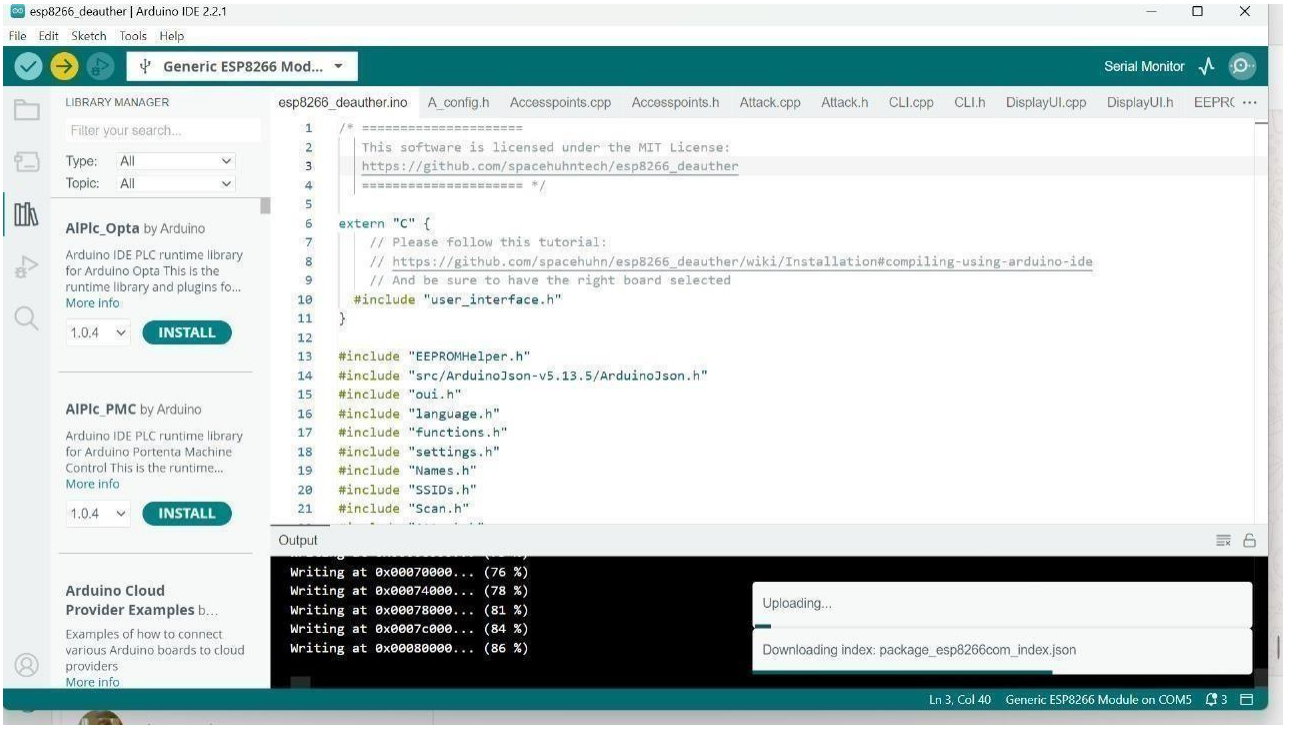


Fig:6.4 uploading the code to esp8266

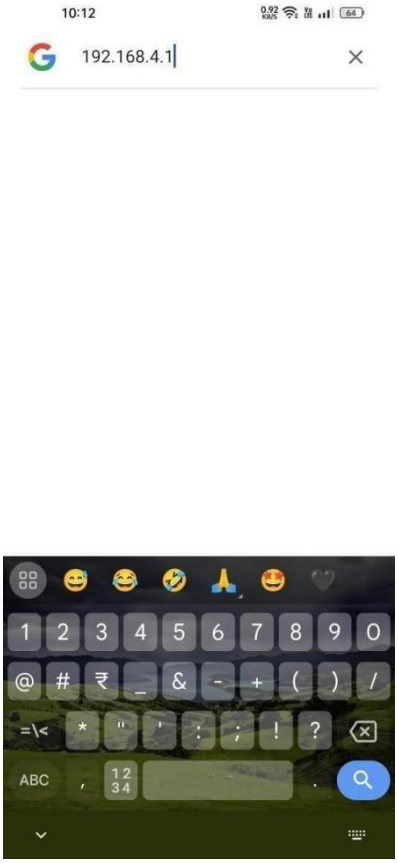


Fig: 6.5 opening 192.168.4.1 by connecting to the esp8266

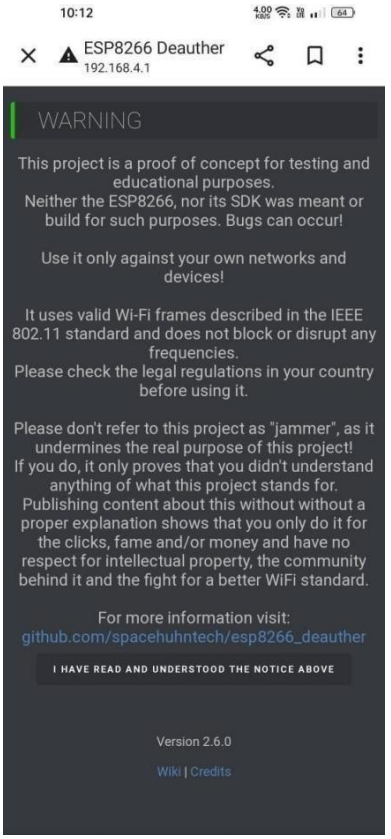


Fig:6.6 select the I understand option

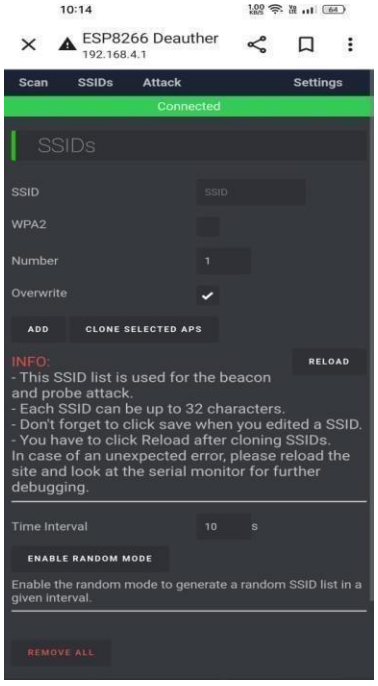


Fig:6.7 select the target ap

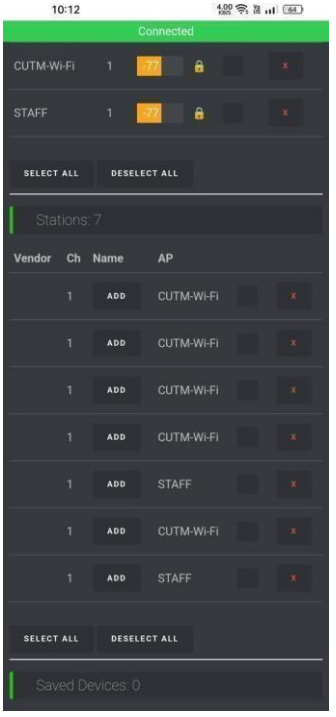


Fig:6.8 create any fake ap's if required

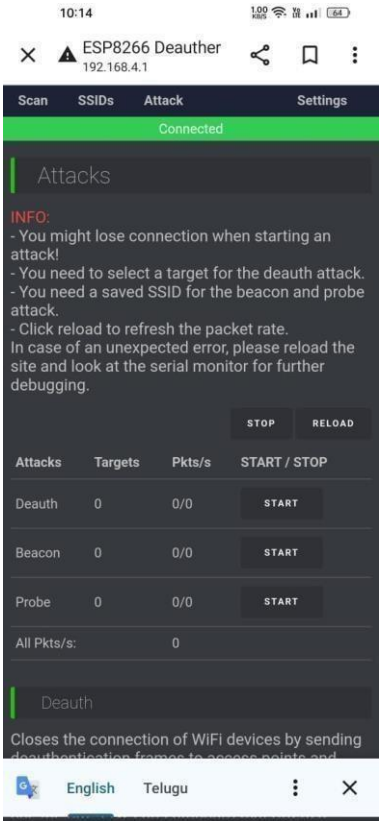


Fig:6.9 start the attack

CONCLUSION

This focuses on developing a user-friendly interface for conducting denial-of-service (DoS) attacks on access points using readily available tools such as the ESP8266 and a data cable. The primary objective is to overload targeted access points with duplicate and extraneous data, rendering them temporarily inoperable and disrupting connectivity for existing users. By creating an accessible interface, users with minimal technical expertise can select their desired target and execute the attack effortlessly. To overload the data frames with duplicate and waste data to the access-point selected and make it not workable to any active user. This will also disconnect the already connected users from accessing the access-point. In this we are to make an user-friendly interface to select the target and perform the attack using the simple tools like ESP8266 and a Data cable. This project delves into the realm of network security, focusing on the design and implementation of a user-friendly interface to conduct denial-of-service (DoS) attacks on access points. Leveraging the simplicity and accessibility of tools such as the ESP8266 microcontroller and a data cable, the project aims to highlight the potential risks associated with lax security measures in commonly used wireless networks.

FUTURE ENHANCEMENT

We want to make this device user-friendly to use. And make the security tests of the wi-fi networks in an easy and simple way. This user-friendly interface allows the users to perform security tests on the selected access-point's . The aforementioned project lies in its potential evolution into a robust and versatile tool for advancing network security practices. First and foremost, future developments could focus on the refinement of the user interface and functionality, aiming for a seamless and intuitive experience for users from diverse backgrounds. Enhancements could include the incorporation of machine learning algorithms to dynamically adapt to evolving attack patterns, providing a more adaptive and resilient defense against denial-of-service attacks. Additionally, the project could expand its capabilities to simulate a wider range of security threats, offering organizations a comprehensive platform to test and fortify their networks against various cyber threats beyond traditional denial-of-service scenarios.

REFERENCES

[1] Junxian Huang, Freng Qian et al, “A close examination of performance and power characteristics of 4G LTE networks”. MobiSys '12 Proceedings of the 10th international conference on Mobile systems, applications, and services, pp 225-238, June 2012

[2] Thuc D. Nguyen, Duc H. M. Nguye, et al, “A Lightweight Solution for Defending Against Deauthentication/Disassociation Attacks on 802.11 Networks”, Vietnam National University, Hochiminh City, University of Texas at Dallas, Richardson, TX, USA, 2012

[3] Milliken, J, Queens Univ. Belfast et al, “Impact of Metric Selection on Wireless Deauthentication DoS Attack Performance”, IEEE Explore , 2(5), pp. 571 – 574, 2013.

[4] David Cossa, “The Dangers of Deauthentication Attacks in an Increasingly Wireless World”, Iowa StateUniversity, 2014

[5] Chibiao Liu and James Yu, “Rogue Access Point Based DoS Attacks against 802.11 WLANs", School of CTI,
DePaul University, 2013

[6] Aslam M. Islam and S.Khan, “802.11 Disassociation DoS Attack and Its Solutions”, A Survey in proceedingof the First Mobile Computing and Wireless Communication international conference , pp. 221-226, 2006

[7] Leandro Meiners, “But...My Station is Awake! (Power Save Denial of Service in 802.11 Networks”, September, 2009

[8] Jie Yang,Yingying et al, “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks” , IEEE Transection on Parallel and Distributed System, 2013

[9] Md. Sohail Ahmad and Shashank Tadamadia,”Short paper: security evaluation of IEEE 802.11w specification”, Proceedings of the fourth ACM conference on Wireless network security, pp 53-58, 2011

[10] Aircrack-ng suite official website http://www.aircrack-ng.org/

[11] Wireshark Network Analyzing tool Available: https://www.wireshark.org/

[12] Nisha Sharma, “Study of DoS Attacks on IEEE 802.11 WLAN and its Prevention/Detection Techniques”, International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 3, 2014

[13] Mishra, V. and Jangale, S, “Analysis and comparison of different network simulators”, on International Journal of Application or Innovation in Engineering & Management, 2014

[14] Joshua Wright and Johny Cash. Hacking Exposed Wireless: Secrets & solutions Book.2015

[15] Arockiam and Vani. A comparative study of the available solutions to minimize Denial of