॥वसुधैव कुटुम्बकम्॥

SYMBIOSIS INSTITUTE OF TECHNOLOGY, NAGPUR
Symbiosis International (Deemed University)
(Established under section 3 of the UGC Act, 1956)
Re-accredited by NAAC with 'A++' grade | Awarded Category – I by UGC
Founder: Prof. Dr. S. B. Mujumdar, M. Sc., Ph. D. (Awarded Padma Bhushan and Padma Shri by President of India)

DEVELOPMENT OF BLUETOOTH JAMMER USING ESP32 AND NRF24L01

GROUP MEMBERS: -

SR NUMBER	NAME OF STUDENTS	PRN NUMBER
1	Swarnim Diwan	24070521126
2	Vivan Tiwari	24070521133
3	Soumya Yedke	24070521124
4	Tilak Barapatre	24070521079

INTRODUCTION

Bluetooth technology operates within the 2.4 GHz ISM (Industrial, Scientific, and Medical) band and is widely used for wireless communication between devices like smartphones, speakers, headphones, and more. However, due to its openness and the nature of radio waves, Bluetooth is susceptible to interference. Bluetooth jamming is a technique that involves the intentional transmission of signals to disrupt or block Bluetooth communications.

In this project, we aim to design and build a Bluetooth jammer using an ESP32 microcontroller and an NRF24L01 wireless transceiver module. The ESP32 is a powerful microcontroller with built-in Wi-Fi and Bluetooth capabilities, and the NRF24L01 is a low-cost transceiver that operates at 2.4 GHz. Together, these devices can be programmed to generate and transmit signals that interfere with Bluetooth communication within a specific range.

This project is intended solely for educational and research purposes. It provides an opportunity to understand wireless communication protocols, the vulnerabilities in Bluetooth communication, and the legal and ethical considerations of signal jamming.

COURSE OUTCOMES:

- Gain an in-depth understanding of how Bluetooth communication works and how it can be interfered with.
- Learn how to interface and program the ESP32 microcontroller with the NRF24L01 module using SPI communication.
- Develop skills in designing and assembling electronic circuits for RF applications.
- Understand the real-world implications of wireless security vulnerabilities and the ethical use of jamming devices.

LITERATURE REVIEW:

To develop a functional Bluetooth jammer, various online resources and literature were consulted. These include:

- NRF24L01 Datasheet: Provided crucial information on frequency, power, and SPI interfacing.
- ESP32 Technical Documentation: Offered insights into GPIO configuration, SPI protocol, and power management.
- GitHub Repositories: Several open-source projects were reviewed to understand implementation strategies for jamming using NRF24L01.
- Academic Papers: Research on RF jamming, packet flooding, and denial-of-service (DoS) attacks in wireless networks.
- Online Forums: Platforms like Arduino Forum and Stack Overflow were helpful for troubleshooting and understanding practical challenges.

WEBSITE CONSULTANT

To extend the scope of our project and provide a structured platform for awareness, documentation, and ethical education, we designed a conceptual website as a **consultant hub** for Bluetooth security.

Purpose of the Website:

- To inform users about Bluetooth vulnerabilities.
- To demonstrate how Bluetooth jamming works (in a legal, educational context).
- To provide guides and resources for ethical hacking, wireless security, and DIY electronics.
- To advise users on legal implications and safe practices regarding RF jamming.

METHODOLOGY / WORKING:

The main objective of this project is to create a device capable of interfering with Bluetooth signals within a defined range using minimal hardware components. The working methodology involves the following key steps:

1. **Component Selection and Assembly:**
   - The ESP32 microcontroller was chosen for its wireless capabilities and compatibility with the NRF24L01 module.
   - The NRF24L01 was selected for its ability to operate in the 2.4 GHz frequency, which is the same range used by Bluetooth.
   - Components were connected on a breadboard, with proper power regulation using an AMS1117 3.3V regulator and a 10uF capacitor for voltage stability.
2. **Hardware Connections:**
   - NRF24L01 was interfaced with ESP32 via SPI protocol.
   - A 3.3V power supply was provided to the NRF24L01 using a linear voltage regulator.
   - Pins used: CE (D4), CSN (D5), SCK (D18), MOSI (D23), MISO (D19), GND, and VCC.
3. **Programming the ESP32:**
   - Using the Arduino IDE, a program was written that initializes the NRF24L01 in transmit mode.
   - The code loops to send random or malformed packets across multiple frequencies in the Bluetooth band (2402 MHz to 2480 MHz).
   - This rapid transmission floods the RF space, causing interference with Bluetooth communications.

4. **Testing and Validation:**
    - The device was tested in a controlled lab setting.
    - Bluetooth devices within a 1–3 meter radius showed connection issues, pairing failures, or intermittent disconnections.
    - The setup was monitored for heating and power stability.
5. **Safety and Ethical Considerations:**
    - The device was only used in a restricted and authorized environment.
    - No interference was directed towards public or unauthorized networks.
    - All work was conducted under academic supervision.

Components Used:

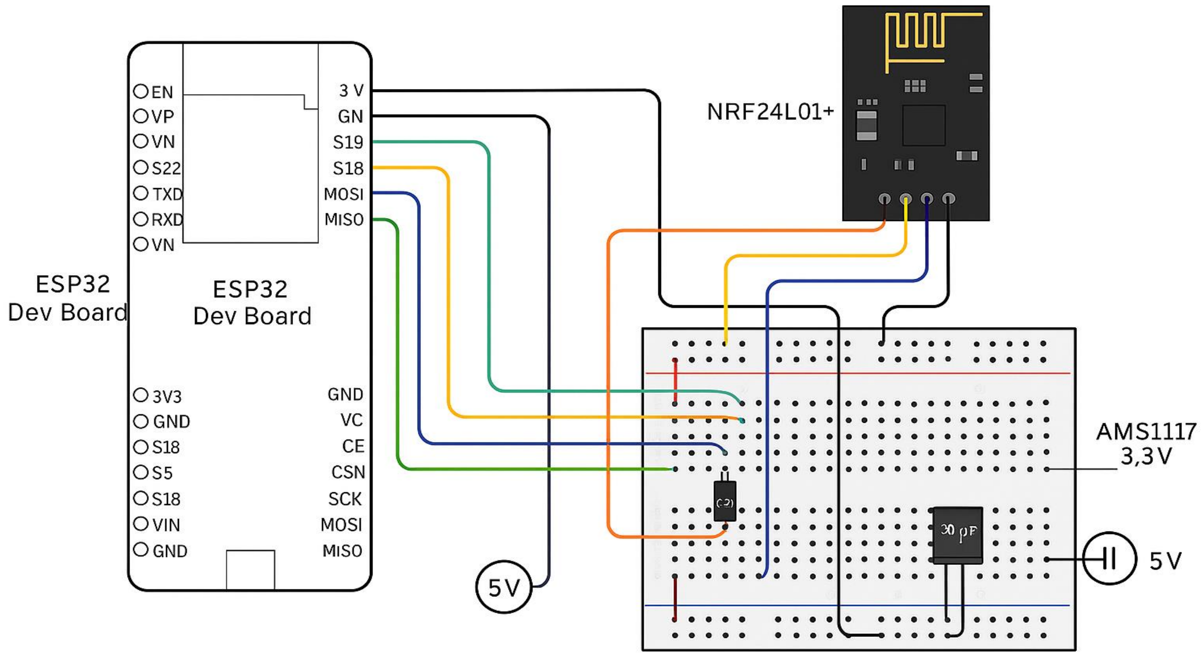
Sr. No.	Item	Description
1	ESP32 Dev Board	32-bit microcontroller with Wi-Fi and Bluetooth
2	NRF24L01	2.4GHz wireless transceiver
3	AMS1117	3.3V Voltage Regulator for stable power supply
4	Breadboard & Jumpers	For circuit assembly
5	Capacitors	10uF electrolytic capacitor for voltage stability
6	USB Cable/Power Supply	To power the ESP32 board

WORKING PRINCIPLE:

1. The ESP32 initializes the NRF24L01 module through SPI communication.
2. Once initialized, the ESP32 sends rapid bursts of data or malformed packets across a range of Bluetooth channels (2402 MHz to 2480 MHz).
3. These transmissions interfere with ongoing Bluetooth communications by flooding the bandwidth.
4. As a result, Bluetooth devices in the vicinity are unable to pair or maintain stable connections.
5. The entire process is continuous until the jammer is turned off or reset.

CIRCUIT DIAGRAM:

Bluetooth Jammer using ESP32 and NRF24L01



The NRF24L01 module is connected to the ESP32 using the following pin configuration:

NRF24L01 Pin	ESP32 Pin
VCC	3.3V (regulated)
GND	GND
CE	GPIO 4
CSN	GPIO 5
SCK	GPIO 18
MOSI	GPIO 23
MISO	GPIO 19

A 10uF capacitor is placed between VCC and GND near the NRF24L01 to prevent voltage dips. The AMS1117 regulator ensures a constant 3.3V supply to the transceiver, which is essential for its proper functioning.

OUTPUT:

- Devices within a range of 1–3 meters experienced significant Bluetooth disruptions.
- Pairing attempts between devices failed while the jammer was active.
- Audio streaming and file transfers over Bluetooth were interrupted.
- The onboard LED (if programmed) blinks to indicate active jamming.

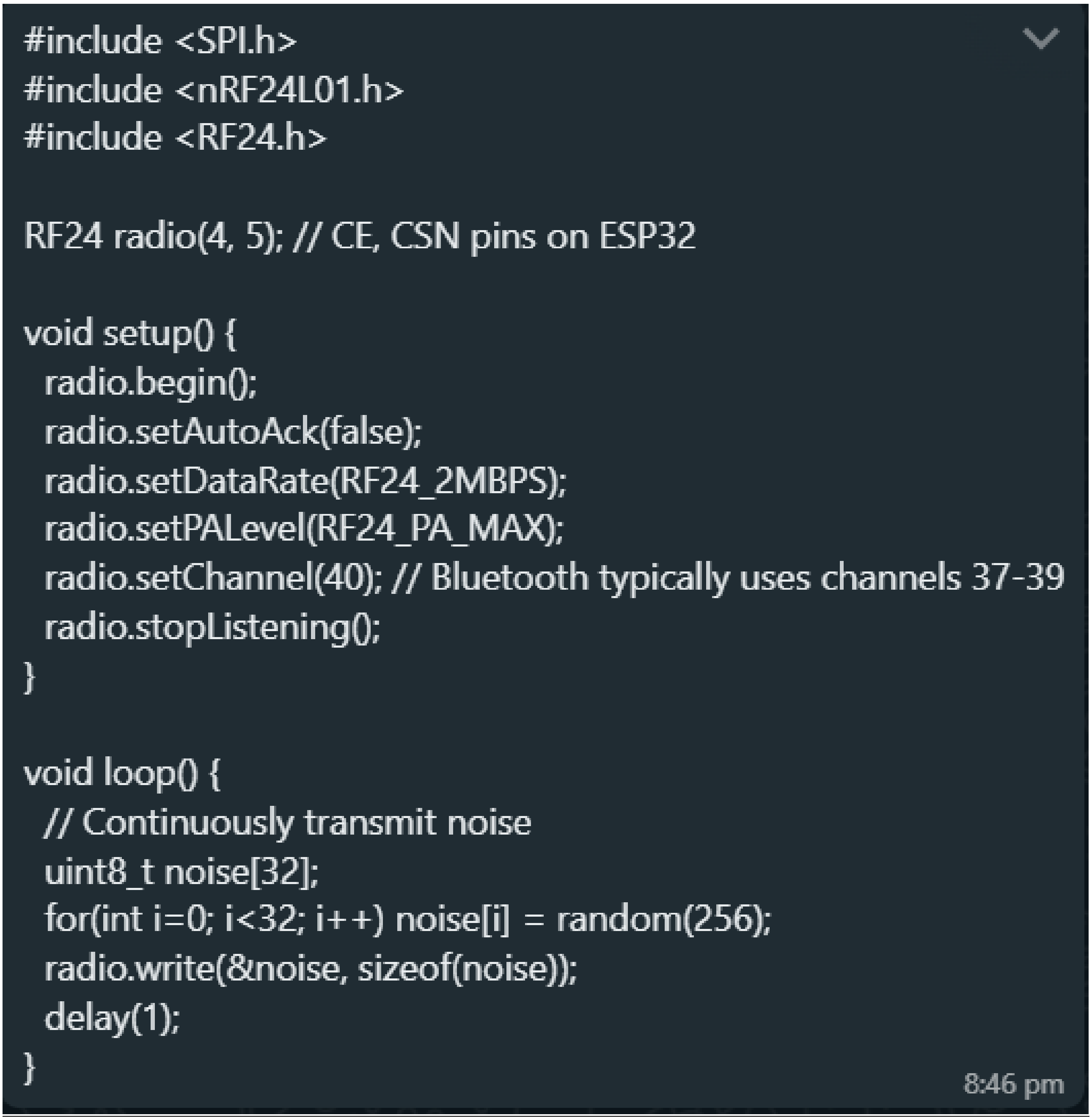
KEY OBSERVATIONS:

- The NRF24L01 is highly sensitive to power fluctuations; using a capacitor is essential.
- The jammer is most effective in close-range environments due to the low-power nature of the NRF module.
- Prolonged jamming can overheat the module; short, timed bursts are recommended.
- Legal regulations prohibit unauthorized jamming in public; usage must be confined to controlled environments for academic testing.

CONTRIBUTIONS:

Name	**PRN**	**Contribution**
Swarnim Diwan	2407052126	Designed the circuit and programmed ESP32
Vivan Tiwari	2407052133	Managed interfacing and testing setup
Soumya Yedke	24070521124	Documented the project and created diagrams
Tilak Barapatre	2407052079	Troubleshooting and performance analysis

CODE USED :-



```
#include <SPI.h>
#include <nRF24L01.h>
#include <RF24.h>

RF24 radio(4, 5); // CE, CSN pins on ESP32

void setup() {
  radio.begin();
  radio.setAutoAck(false);
  radio.setDataRate(RF24_2MBPS);
  radio.setPALevel(RF24_PA_MAX);
  radio.setChannel(40); // Bluetooth typically uses channels 37-39
  radio.stopListening();
}

void loop() {
  // Continuously transmit noise
  uint8_t noise[32];
  for(int i=0; i<32; i++) noise[i] = random(256);
  radio.write(&noise, sizeof(noise));
  delay(1);
}
```

8:46 pm

CONCLUSION:

This project successfully demonstrated the feasibility of building a Bluetooth jammer using ESP32 and NRF24L01. Through this experiment, we gained insights into wireless communication vulnerabilities, hardware interfacing, and RF transmission. The practical challenges encountered during testing improved our problem-solving and circuit debugging skills. This project also highlighted the importance of ethical considerations and legal constraints surrounding the use of jamming technologies.

Prof. Ankita Avthankar

Course Teacher

LAB Incharge