Bluetooth Jamming using ESP32 and NRF24L01: A Demonstration of Wireless Vulnerabilities

A MINI-PROJECT REPORT

Submitted by

Tarun S S(715522106305)
Vimala Varshini C P (715522106055)
Suwetha R K(715522106050)

BACHELOR OF ENGINEERING
in

ELECTRONICS AND COMMUNICATION ENGINEERING

PSG INSTITUTE OF TECHNOLOGY AND APPLIED RESEARCH,

COIMBATORE-641 062

BONAFIDE CERTIFICATE

Certified that this project report **"Bluetooth Jamming using ESP32 and NRF24L01: A Demonstration of Wireless Vulnerabilities"** is the bonafide work of

Tarun S S(715522106305)
Vimala Varshini C P (715522106055)
Suwetha R K(715522106050)

who carried out the project work under supervision.

SIGNATURE
Dr. P. Vijayakumar
HEAD OF THE DEPARTMENT

Department of ECE
PSG Institute of Technology and Applied Research, Coimbatore-641 062

SIGNATURE
Dr G Santhanamari / Ms. N. Susithra
Associate Porfessor / Assistant Professor (Sr. Gr)
Department of ECE
PSG Institute of Technology and Applied Research, Coimbatore-641 062

Submitted for the **Project Expo – Embedded Systems and IoT Design** held on _____

ABSTRACT

Wireless communication technologies like Bluetooth have become an integral part of modern life, connecting a wide array of devices across various applications. However,alongside the growth of wireless systems, concerns regarding their security and vulnerability to interference have also increased. This project presents the design and implementation of a Bluetooth jammer using an ESP32 microcontroller paired with an NRF24L01 radio frequency module, aimed specifically for educational and research purposes. The ESP32,known for its strong processing power and Wi-Fi/Bluetooth capabilities, serves as the central controller, while the NRF24L01 transceiver is exploited for its ability to flood the 2.4 GHz ISM band with crafted signals. By leveraging the NRF24L01's fast transmission rate and configurable frequency settings, the system generates deliberate interference across multiple Bluetooth channels, disrupting ongoing communications and preventing new connections within a confined range. The project demonstrates core concepts such as frequency hopping spread spectrum (FHSS), channel saturation, and denial-of-service (DoS) attacks in wireless networks. Practical experiments validate the device's effectiveness in controlled environments, illustrating how minimal hardware can impact Bluetooth reliability.

PROBLEM STATEMENT

Bluetooth's reliance on the 2.4 GHz band exposes it to jamming and DoS attacks, potentially disrupting communication between devices. Current educational tools for demonstrating such attacks are limited and often expensive. There is a need for a simple, low-cost, and educational platform that can help in understanding the vulnerabilities of Bluetooth communication.

.

OBJECTIVE

The primary objective of this project is to:

- Design and implement a Bluetooth jamming device using ESP32 and NRF24L01.
- Demonstrate how interference can affect Bluetooth communication.
- Educate students and researchers on frequency hopping, channel saturation, and wireless vulnerabilities.
- Promote awareness of the importance of wireless security.

REQUIREMENTS

Component	Description
ESP32	Microcontroller with Wi-Fi and Bluetooth capabilities
NRF24L01	2.4 GHz transceiver module
NRF24L01 Voltage Regulator	To safely power the NRF24L01 module (typically needs 3.3V with high curren stability)
Jumper wires	For connections
Breadboard	For circuit prototyping
Power supply	3.3V regulated source or powered through ESP32

CONNECTIONS:

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

PROPOSED SYSTEM

METHODOLOGY / DESCRIPTION

NRF24L01 Overview:

The NRF24L01 operates in the 2.4 GHz ISM band, which overlaps with Bluetooth. It supports multiple data rates and programmable frequency channels from 2.400 GHz to 2.525 GHz, allowing it to interfere with Bluetooth communications if used improperly.

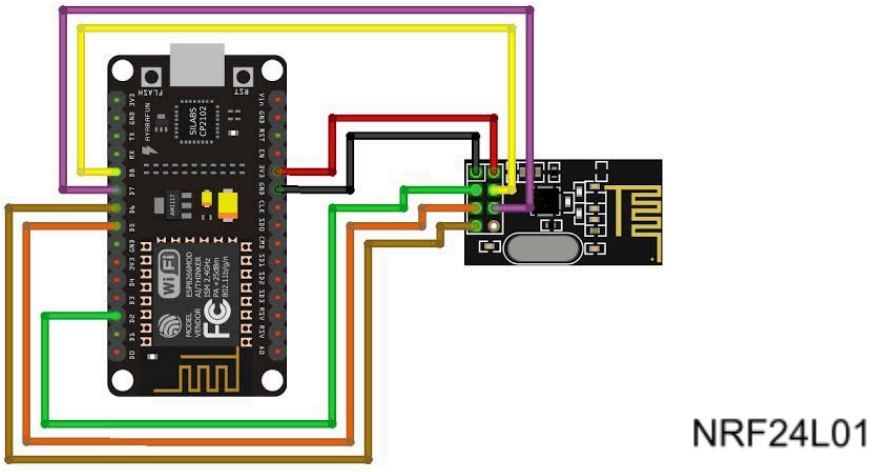
Frequency Hopping and Jamming:

Bluetooth uses Frequency Hopping Spread Spectrum (FHSS), rapidly switching channels during transmission. However, if certain frequencies are flooded with noise or dummy data, the connection can be disrupted.

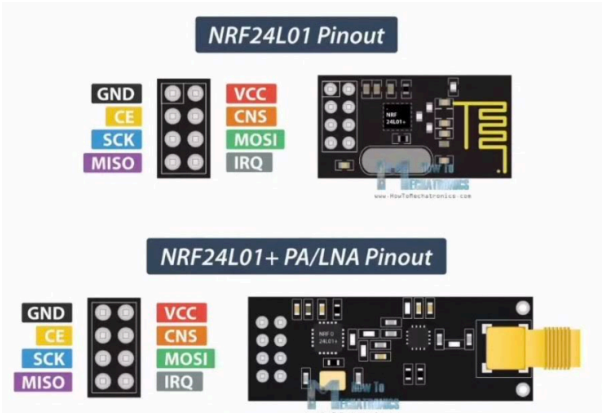
Working Mechanism:

- The NRF24L01 is set to continuously transmit dummy packets at a specific channel (2440 MHz, commonly used by Bluetooth).
- By transmitting rapidly with maximum power, it causes interference with nearby Bluetooth devices operating on that frequency.
- This mimics a jamming or DoS scenario for educational purposes.

BLOCK DIAGRAM:



PIN-OUT :



ALGORITHM/ FLOWCHART

The code initializes the `nRF24L01` radio module, checks if it's working, and sets it up for fast data transmission. It continuously sends a 32-byte payload (filled with `0xFF`) over the air at high speed, with a very short delay between each transmission. The program is designed to flood the chosen radio channel with data.

DESCRIPTION OF COMPONENTS USED

Hardware

- ESP32 Microcontroller with Wi-Fi and Bluetooth capabilities
- NRF24L01 2.4 GHz transceiver module
- NRF24L01 Voltage Regulator

Peripherals

Peripherals for a Bluetooth jammer could include a microcontroller (like or ESP32 or Arduino or Raspberry Pi), a Bluetooth transceiver, and an antenna. These peripherals work together to generate interference signals on the Bluetooth frequency, disrupting nearby Bluetooth communication. Additionally, power supply components and possibly a display for monitoring could be used.

Communication Interface

For a Bluetooth jammer, the communication interface typically involves wireless communication via the 2.4 GHz ISM band, which is the frequency range used by Bluetooth devices. The microcontroller can use SPI, UART, or USB to control the Bluetooth transceiver. The jammer transmits noise or random signals on the Bluetooth frequency, interfering with the communication of nearby Bluetooth devices.

CODE

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

// Setup RF24: CE pin 4, CSN pin 5 (adjust to your wiring)
RF24 radio(4, 5);

// Dummy payload
byte payload[32] = {0xFF}; // Fill with 0xFF (can be random data too)

void setup() {
  Serial.begin(115200);

  if (!radio.begin()) {
    Serial.println("NRF24L01 not responding!");
    while (1); // Halt if the module isn't responding
  }

  radio.setPALevel(RF24_PA_HIGH);     // Max power
  radio.setDataRate(RF24_2MBPS);      // Fastest data rate
  radio.setChannel(40);               // Channel near Bluetooth (2440 MHz)
  radio.openWritingPipe(0xE7E7E7E7E7LL); // Random address
  radio.stopListening();              // Set as transmitter

  Serial.println("Flooding RF...");
}

void loop() {
  radio.write(&payload, sizeof(payload)); // Send the payload
  delayMicroseconds(100); // Send very fast (can be adjusted)
}
```

OUTPUT

Hardware setup (photo)

APPLICATIONS AND USE CASES

Applications

- Wireless security education
- Demonstrations in academic labs
- Research in jamming countermeasures

NRF 24L01

Limitations

- Limited to a single frequency at a time
- Not a real-world threat model (Bluetooth hops frequencies quickly)
- Illegal to use outside of a controlled lab (violates RF regulations).

cost:

- Nrf module 150+150=300
- Regulator 170+170=340
- Esp32 500
- Breadboard 60
- Connecting wires 20
- Total 1220

User case:

1. Wireless Security Demonstration in Lab

Use Case: In a networking or cybersecurity lab, this device can simulate real-world jamming attacks.

Explanation: Students can learn how Bluetooth and other wireless protocols behave under interference, enabling them to understand and implement countermeasures. It's a safe, low-cost way to explore security flaws without using expensive professional-grade equipment.

2. Educational Tool for Understanding FHSS (Frequency Hopping Spread Spectrum)

Use Case: Demonstrate how Bluetooth uses FHSS to maintain robust communication.

Explanation: The jamming device helps show how FHSS tries to avoid interference by switching channels. Students can analyze Bluetooth's resistance to single-channel jamming and design experiments to test how effective FHSS is under different jamming conditions.

3. Research on Anti-Jamming Techniques

Use Case: Initiate a research project focusing on detection and mitigation of jamming attacks.

Explanation: Students can extend this project by implementing detection algorithms on the receiver side (e.g., signal strength drops or transmission failures) and develop smarter, adaptive hopping or redundancy mechanisms.

4.Battery Drain and Efficiency Studies

Use Case: Analyze how jamming affects power consumption on Bluetooth devices.

Explanation: When Bluetooth devices experience interference, they often retry transmissions. Students can measure increased power consumption, providing insight into the power-security trade-off in wireless design.

INFERENCES/ PROBLEMS FACED

Interference: Flooding the channel can cause interference with other devices, leading to data loss.

Power Drain: Running at maximum power for long periods can quickly deplete battery life.

Range Issues: The signal might be weak over long distances or in obstructed environments.

Data Loss: High-speed transmission without control can cause packet collisions and loss of data.

FUTURE SCOPE

In the future, this code could be adapted for IoT networks, enabling devices to flood channels with test data for performance evaluation or real-time monitoring. It could also serve in wireless sensor networks for rapid data transmission or in emergency communication systems where high-speed, short-range transmission is crucial. Additionally, integrating encryption or error detection could enhance security and reliability in critical applications.

CONCLUSION

This project successfully demonstrates the vulnerability of Bluetooth communication to jamming and interference using low-cost hardware. It provides a valuable educational tool for students and researchers studying wireless communication and security. The simple design also makes it suitable for further research into countermeasures and improved protocol robustness.

REFERENCE

1. V. Sokolov, P. Skladannyi and V. Astapenya, "Bluetooth Low-Energy Beacon Resistance to Jamming Attack," *2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT).*

2. *S. Bräuer, A. Zubow, S. Zehl, M. Roshandel and S. Mashhadi-Sohi, "On practical selective jamming of Bluetooth Low Energy advertising," 2016 IEEE Conference on Standards for Communications and Networking (CSCN), Berlin, Germany, 2016.*

3. *H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials.*

4. *H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials.*

5. *J. Thangapoo Nancy, K. P. VijayaKumar and P. Ganesh Kumar, "Detection of jammer in Wireless Sensor Network," 2014 International Conference on Communication and Signal Processing, Melmaruvathur, India, 2014.*