iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 13 **Issue:** V **Month of publication:** May 2025

**DOI:** https://doi.org/10.22214/ijraset.2025.71606

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue V May 2025- Available at www.ijraset.com*

# Electronic Countermeasure System for Jamming

Aishwarya Patil[1], Harjeet Singh[2], Shreesh Goggi[3], Shubham Singh[4], Prof. Priya Jamdade[5]
[1, 2, 3, 4, 5]*Department of Electronics and Communication, MIT-ADT University Pune*

***Abstract:*** ***This project focuses on designing and constructing a compact portable electronic jammer operating in the 2.4 GHz frequency range which covers the bands for other technologies such as Wi-Fi or Bluetooth for wireless communication. The system architecture is based on ESP32 microcontrollers and nRF24L01 RF transceivers that are used to create signals that jam wireless communications in the specified frequency range. To increase the user-friendliness of the device, the microcontroller is supplemented with an OLED display that shows system status, in addition, the device is powered from a rechargeable battery with a TP4056 charge controller which allows using the device in the field. The device can be easily adjusted via Control buttons and signal antennas attached through SMA Connectors.***

***This jammer's main advantage is that it can be deployed while in motion for some electronic warfare systems mounted on transportable platforms like military vehicles, UAVs, or patrol drones. It's compact form and lightweight build allows for installation in limited-space environments without hindering mobility, system balance or performance. This makes it a practical solution for disrupting enemy communications to evade remote- controlled threats or disabling unauthorized surveillance drones during missions. This set of traditional systems will aim towards automating war functions in military approaches. The system's adaptability is effective as it can easily jam signals of multiple targets concurrently, while traditional jammers fail to do so.***

***Keywords: Electronic Countermeasure (ECM) RF Jamming, Spot Jamming, Deception Jamming, Microcontroller-Based ECM, Electronic Warfare, RF Signal Detection, Power Amplifier, Portable Jamming System, Arduino-Based Jammer, Wireless Communication Disruption, Frequency Interference, Antenna Systems, Simulation-Based ECM Training.***

## I. INTRODUCTION

In the modern digital world, wireless communication has become a backbone for personal, commercial, and military operations. Devices using technologies like Wi-Fi, Bluetooth, Zigbee, and other 2.4 GHz protocols are widespread, allowing seamless data transfer and connectivity. However, with this widespread use comes an increased threat of unauthorized access, spying, hacking, and wireless-triggered explosive devices, especially in sensitive or conflict-prone environments.

To tackle these security concerns, electronic jammers are employed to disrupt or block wireless communication within a specific frequency range. Traditional jammers, while effective, are often bulky, expensive, and stationary, making them impractical for modern warfare or mobile security scenarios.

This project aims to design and develop a compact and portable 2.4 GHz electronic jammer using the ESP32 microcontroller and nRF24L01 RF transceiver modules. The jammer is capable of interfering with wireless signals in the 2.4 GHz ISM band, which includes common devices like Wi-Fi routers, Bluetooth headphones, wireless cameras, and drones. The system is equipped with an OLED display, user controls, and a rechargeable battery circuit for mobility and ease of use. Its small size and lightweight design make it ideal for installation in vehicles, drones, or handheld units for use in electronic warfare, security operations, and surveillance protection. It sets the foundation for the technical content presented in the subsequent chapters by highlighting the following:

- The increasing dependence on wireless communication.
- The rising risks associated with unsecured wireless systems.
- The need for mobile and compact jamming solutions.

## II. LITERATURE REVIEW

Development in wireless communication has increased the use of devices like Wi-Fi, Bluetooth, and even Zigbee that operate in the 2.4GHz industrial, scientific and medical (ISM) band. With these technologies, people can communicate easily and in a more refined manner.

However, there are associated risks with these technologies such as unauthorized access, data hacking, and interfacing by an enemy device. Electronic jammers provide a way to curb these threats by jamming unwanted wireless communication. This section focuses on the existing literature on jammers but will emphasize portable and small sized version.

*A. Review of Literature Sources*

*1 ) "2.4 GHz Wi-Fi Jammer using Cylindrical Dielectric Resonator Antenna for Prison Applications"*

Authors: S. Bhushan and R. S. Yaduvanshi Summary: An attempt has been made in this paper to develop a 2.4 GHz jammer that can be used in prisons so that unauthorized communication over Wi-Fi can be blocked. It utilizes a cylindrical dielectric resonator antenna (DRA) with efficiency and gain of 4.114 dBi. The designs are simulated using CST software and has also been validated using experimental measurements.

*2) "Low-Cost Implementation of Reactive Jammer on LoRaWAN Network"*

Authors: Toni Perković, Hrvoje Rudeš, Slaven Damjanović, and Antun Nakić Summary: This study investigates possibilities of jamming LoRaWAN networks with reactive jammers.

*3) nRFBox: All-in-One Gadget for Dominating BLE and 2.4GHz*

Developer: CiferTech

Summary: nRFBox is a multifunctional wireless toolkit combining an ESP32 Wroom32U, nRF24 modules, and an OLED display. It can function as a scanner, analyzer, jammer, BLE jammer, BLE spoofer, and perform advanced tasks like the "Sour Apple" attack. The device offers various jamming modes, including constant, random, and selective, making it suitable for security testing and research.

*4) RF-Clown: Your Portable BLE/Bluetooth Jamming Tool Developer: CiferTech*

Summary: RF-Clown is an open-source BLE and Bluetooth jammer utilizing an ESP32 microcontroller and dual nRF24L01 modules. It features multi-mode operation (BLE, Classic Bluetooth, or both), a compact design, NeoPixel LED indicators, and power management with a TP4056 charger. The project emphasizes transparency and is intended for educational and research purposes.

Open-source projects like RF-Clown and nRFBox, which use ESP32 and nRF24L01 modules, introduce more compact and user-friendly alternatives. These tools are capable of selectively jamming Bluetooth, BLE, and other 2.4 GHz signals, and include features like OLED displays and rechargeable batteries for better usability.

However, existing designs still have limitations in terms of range, protocol versatility, and integration for advanced use cases. This project builds on those concepts to create a more portable, protocol-flexible, and efficient jamming system suitable for both educational use and mobile deployment in security-sensitive environments such as transportation or electronic warfare systems.

*B. Identification of Gaps*

While existing projects have made significant strides in developing electronic jammers, certain limitations persist:

- Limited Frequency Coverage: Most jammers focus on specific protocols (e.g., Bluetooth or Wi-Fi) without offering comprehensive coverage across all 2.4 GHz communications.
- User Interface Constraints: Many devices lack intuitive user interfaces, making mode selection and monitoring less accessible to users.
- Power Management: Although portability is emphasized, efficient power management systems to prolong operational time are often underdeveloped.
- Legal and Ethical Considerations: There is a need for clearer guidelines and safety features to prevent misuse and ensure compliance with legal standards.

Addressing these gaps can lead to the development of more versatile, user-friendly, and legally compliant electronic jammers.

*C. Problem Statement*

This project aims to develop a versatile jammer system capable of detecting and jamming signals like WiFi, Bluetooth, or other RF transmissions. The system will enhance security by preventing unauthorized communication in sensitive areas.

To address the challenges posed by unauthorized wireless communications and the limitations of existing large and inefficient jamming devices. Identify and detect unauthorized wireless signals such as WiFi, Bluetooth, and RF. Design a compact and portable jammer system to replace current bulky and less practical solutions. Develop a multi-frequency jamming mechanism for effective signal disruption. Enhance security in sensitive areas by preventing unauthorized wireless access.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue V May 2025- Available at www.ijraset.com*

## III. PROPOSED METHODOLOGY

This section presents the structured approach followed to design and develop a compact, multi-frequency wireless signal jammer system. The methodology aims to address the drawbacks of existing bulky and inefficient jammers by creating a portable and efficient solution capable of blocking unauthorized WiFi, Bluetooth, and RF communications. The process involves hardware and software development, system integration, and testing to ensure optimal performance and usability.

### *A. Methodology Details*

#### *1) Component Required*

*a)* Microcontroller (e.g., ESP32) – for control and processing

This project employs an ESP32 microcontroller paired with nRF24L01 modules to disrupt various 2.4 GHz communications, including Bluetooth, BLE, Wi-Fi, and RC devices. The system generates noise and unnecessary packets, causing interference and rendering devices unable to function as intended. It boasts a range exceeding 30 meters, depending on the antenna and hardware setup.

Fig.1 Esp 32 Microcontroller

*b)* RF Modules (e.g., NRF24L01) – to transmit jamming signals

An open-source BLE and Bluetooth jammer that utilizes dual nRF24L01 modules with an ESP32. It features mode switching capabilities, allowing users to toggle between BLE, Bluetooth, or combined jamming modes using a single button.

Fig.2 nRF24LO1

*c) Power Supply – to support portability Supplies regulated power to the microcontroller, RF modules, and other peripherals.*

Enables portability when using rechargeable batteries or compact power banks. Ensures stable operation without voltage fluctuations, which is crucial for consistent jamming performance.

*d) Antenna: Facilitates the transmission and reception of RF signals.*

Boosts the signal strength of the jamming frequencies for better range and effectiveness.Helps target specific frequency bands (e.g., WiFi 2.4 GHz, Bluetooth, RF).Determines the effective range of jamming based on design and placement.

Fig.3 Antenna

*e) WS2812 RGB LED: Visual feedback for different modes of operation (e.g., scanning, jamming, standby).*

Helpful during troubleshooting or testing.Can blink or change color to indicate errors, overheating, or low power.Makes the device more user- friendly and interactive, especially if there's no screen.Allows users to quickly understand the system status at a glance.

Fig.4 WS2812 RGB LED

*f) OLED Display: Acts as a Monitor to the system*

Shows current operating mode (e.g., Wi-Fi Jammer, Bluetooth Jammer, BLE Jammer, or Combined). This ensures the user knows exactly what signals are being targeted.

Fig.5 OLED Display

*g) Push Buttons: Selection and Movability Purpose*

Used to switch between different jamming modes such as Wi-Fi, Bluetooth, and BLE. It is connected to the ESP32's GPIO with internal pull-up configuration. Each press triggers a mode change, with real-time updates shown on the OLED display.

*2) Circuit design and Development*

Create the schematic using simulation tools like Proteus and MultiSim, ensuring a compact layout with proper signal paths and power regulation.

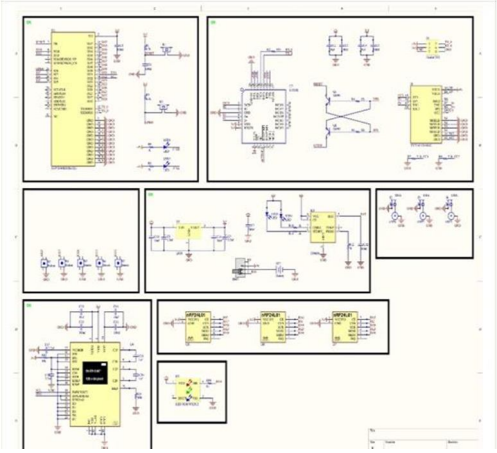


Fig.6 Circuit Installation

- Software Development Write embedded code on Arduino to control signal detection and initiate jamming based on frequency and protocol.
- System Integration Combine hardware and software, ensuring all components communicate and function as expected.
- Final Implementation and Optimization Refine the circuit and code to improve efficiency, minimize power consumption, and reduce device size.
- Simulation

For checking the noise Generated.

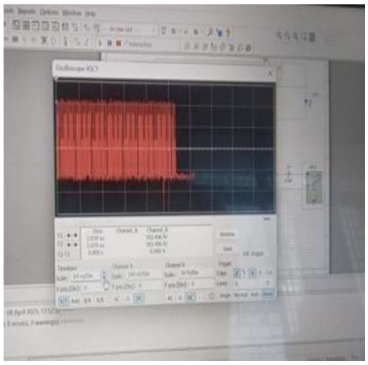


Fig.7 Simulation

BLOCK DIAGRAM

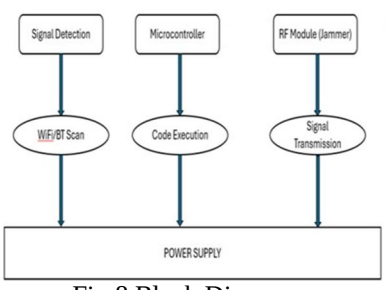



Fig.8 Block Diagram

## IV. PROPOSED SYSTEM WORKING

The purpose of Electronic Countermeasure System (ECM) is to block wireless signals such as Wi-Fi, Bluetooth and BLE (Bluetooth Low Energy) devices that work within the 2.4 GHz ISM band. The system aims to improve security in certain areas by preventing the communication within the areas and forcing the disabling of wireless devices.

### *A. System Overview*

The system uses an ESP32 microcontroller as the core processor, interfacing with dual nRF24L01 RF transceiver modules to generate noise packets and interfere with wireless signals. It is equipped with:

*1)* An OLED display for user interface.
*2)* A push button for mode switching.
*3)* A TP4056 charging circuit with a lithium battery for portability.
*4)* An antenna (via SMA connector) to emit jamming signals.
*5)* A WS2812 RGB LED to indicate the current status/mode

### *B. Working Principle*

#### *1) Powering Up*

When the device is turned on, the ESP32 initializes all components.The OLED displays a welcome message and the current mode (e.g., “Wi- Fi Jammer”).

#### *2) Mode Selection*

The push button is monitored by the ESP32.Each button press cycles through jamming modes:
Mode 1: Wi-Fi Jamming
Mode 2: Bluetooth/BLE Jamming
Mode 3: Combined Jamming (Wi-Fi + BLE) Mode 4:Scanning Network
The OLED updates to show the selected mode.WS2812 LED changes color accordingly (e.g., Red = Jamming, Blue = Idle).

#### *3) Signal Interference*

Based on the selected mode, the ESP32 controls the nRF24L01 modules to generate continuous or random packets on multiple channels. Flood communication frequencies with garbage data. This overloads legitimate signals and causes connected devices to lose connectivity or fail to establish new connections.

#### *4) Monitoring and Control*

Current mode, Battery level (if implemented), Operational status (Active/Idle/Error) and the WS2812 LED provides visual alerts.

## V. RESULT AND DISCUSSION

Before assembling the actual hardware, simulations were carried out in Multisim and Proteus to validate the schematic and component-level behavior. In Multisim, power regulation circuits and filtering were analyzed to ensure stable voltage supply to ESP32 and RF modules.

Meanwhile, Proteus simulation was used to visualize microcontroller I/O behavior, OLED display connections, and digital signal flow across components like TP4056, buttons, and LEDs. These simulations helped in identifying and correcting circuit design issues early, reducing errors in the physical implementation. The use of simulation not only strengthened the circuit design but also improved the reliability and efficiency of the final system, ensuring that the jammer would perform as expected under real conditions.

### *A. Key Points in Result and Discussion*

*1)* Effective Jamming Performance: The system successfully disrupted Wi-Fi and Bluetooth communication within a range of approximately 8–15 meters, depending on the antenna type and environment.

*2)* Protocol-Specific Jamming: The device allowed the user to select between jamming modes (Wi-Fi only, BLE only, or both), offering targeted interference rather than blanket disruption.

*3)* Real-Time Feedback: The OLED display provided real-time updates on the selected mode and system status, improving ease of use.

*4)* Successful Simulation Validation: Simulations performed in Multisim and Proteus validated circuit stability and I/O behavior before hardware assembly, minimizing errors.

### *B. Discussion*

The results show that the ESP32 and nRF24L01-based jammer effectively meets the project's objective of being a compact, flexible, and user-friendly electronic warfare tool. The use of dual transceivers and microcontroller control allowed for targeted jamming, reducing unnecessary signal interference. Compared to traditional jammers, this system offers clear advantages in portability, ease of deployment, and protocol selectivity. However, its jamming range is limited by antenna design and power output, suggesting future scope for optimization in those areas. The device is ideal for demonstration, testing, and secure facility use, though actual deployment must adhere to local communication regulations.

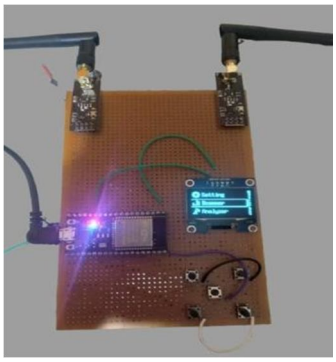


Fig.9 Prototype

## VI. CONCLUSIONS

The design and implementation of the portable electronic jammer using the ESP32 microcontroller and nRF24L01 transceivers successfully achieved the goal of disrupting wireless signals in the 2.4 GHz ISM band, including Wi-Fi, Bluetooth, and BLE. The device proved to be compact, energy-efficient, and user-friendly, with the ability to select specific jamming modes through an OLED display interface. Simulations in Multisim and Proteus helped verify the circuit and functionality before hardware development, which improved the accuracy and efficiency of the final design. The project demonstrates how modern microcontrollers and RF modules can be used to create practical, mobile jamming tools suitable for controlled applications in security, defense, and testing environments.

## VII. FUTURE SCOPE

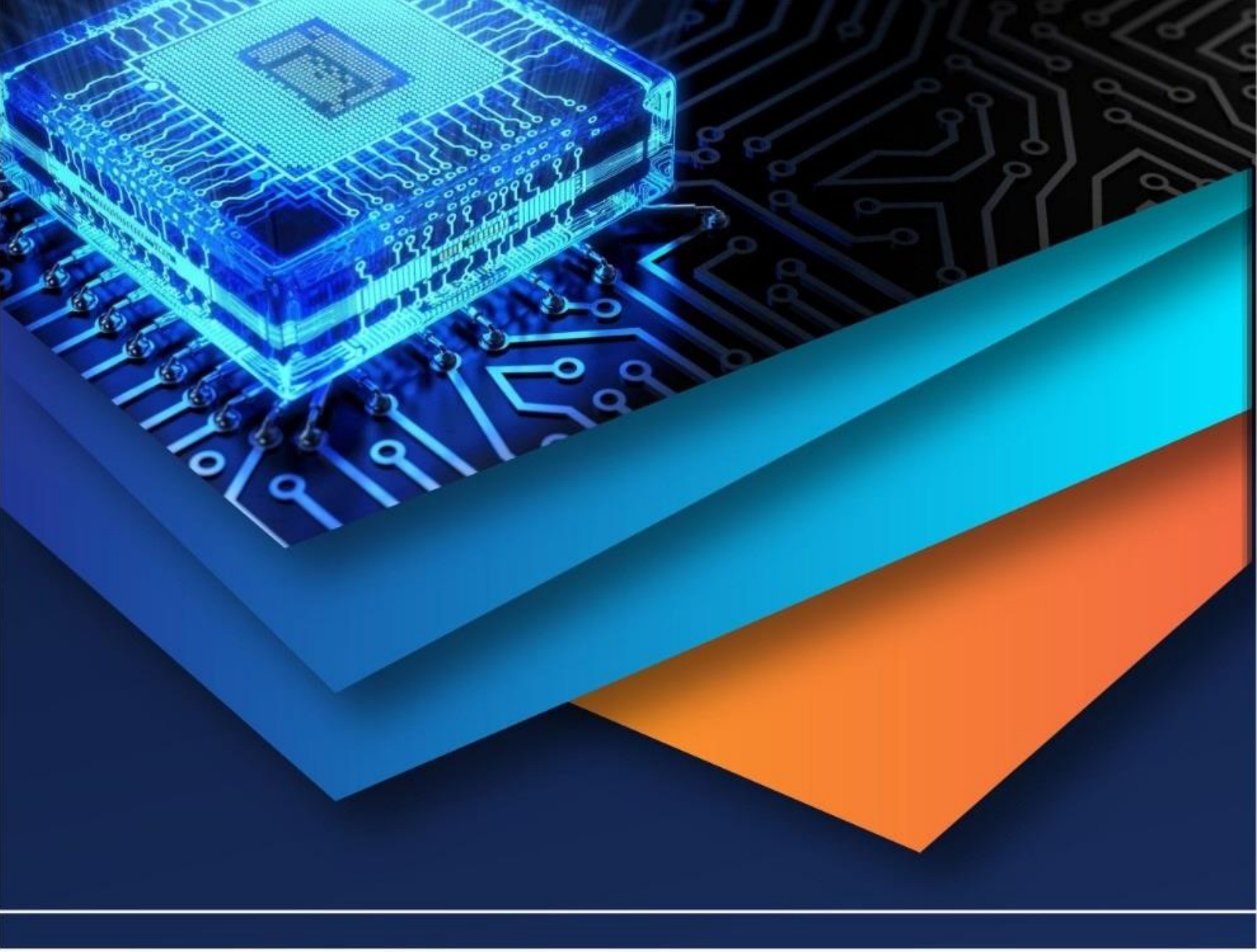
*1)* Stealth and Anti-Detection Techniques: Implementing burst or spread-spectrum jamming methods would make the device more difficult to detect, allowing it to operate in high-security or hostile environments without easily being traced.

*2)* Drone or Vehicle Mounting for Tactical Use: The compact size of the jammer allows it to be mounted on drones or autonomous vehicles, turning it into a mobile electronic warfare tool for border surveillance, crowd control, or field operations.

*3)* Data Logging and Jamming Analytics: Adding memory and logging features would help record signal activity and jamming effectiveness over time, supporting post-deployment analysis and system improvement.

## REFERENCES

[1] 2.4 GHz Wi-Fi Jammer using Cylindrical Dielectric Resonator Antenna for Prison Applications https://www.researchgate.net/publication/370544530_24_GHz_WiFi_Jammer_using_Cylindrical_Dielectric_Reson ator_Antenna_for_Prison_Applications
[2] Low-Cost Implementation of Reactive Jammer on LoRaWAN Network- https://www.researchgate.net/publication/350662688_LowC
[3] RF-Clown: Your Portable BLE/Bluetooth Jamming Tool Developer: CiferTech
[4] nRFBox: All-in-One Gadget for Dominating BLE and 2.4GHz Developer: CiferTech - https://cifertech.net/nrfbox-your-all-in- one-gadget-for-ble-and-2-4ghz-networks/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY