A Secure RFID Sensing Platform Leveraging Self-Jamming for Enhanced Identification

J Jithendranath[1], B. Nandu Priya[2], S. Harika[3], V. Santhosh[4], G. Divya Sree[5], S. Naga Thejesh[6]

*[1]Department, Assistant Professor, Dept. of ECE, ALTS, Anantapuramu

[2,3,4,5,6]UG Scholar, Dept.of ECE, ATLS, Anantapuramu

ABSTRACT

Commodity RFID tags can only backscatter stored EPC codes and lack sensing capabilities. Existing RFID-based sensing platforms often require complex hardware modifications, increasing costs and limiting flexibility. This paper presents a Self-Jamming Identification and Sensing Platform (SJISP), comprising SJISP nodes and a standard RFID reader. The SJISP node integrates a jammer radio module operating at the same frequency as the reader, controlled by a microcontroller (MCU) to selectively interfere with the RFID query process. By switching the jammer on and off, sensing data is encoded as bit 0 and bit 1, respectively, and demodulated via the EPC UHF Gen2 protocol. To enhance energy efficiency, a prefix codebook-based data delivery scheme is implemented, reducing energy consumption by over 50%. Experimental results demonstrate a 99% packet reception rate (PRR) and strong robustness to environmental disturbances. A real-world demo with temperature and light sensors showcases the system's practicality.

Keywords: Backscatter communication, interference signal, modulation, prefix codebook, RFID system, self-jamming, EPC UHF Gen2, sensor integration, energy-efficient communication, microcontroller-based control, jammer radio module, wireless sensing, environmental robustness, real-world deployment, RFID-based sensing platform.

I. INTRODUCTION

The advancement of RFID technology has significantly enhanced automation, asset tracking, and wireless communication across industries such as logistics, healthcare, and security. However, conventional RFID systems face limitations in sensing capabilities and vulnerability to external interference, making them less reliable for critical applications. Existing RFID-based sensing platforms often require costly hardware modifications or complex tag enhancements, restricting scalability and increasing deployment challenges. This study addresses these issues by developing a Self-Jamming Identification and Sensing Platform (SJISP) that enables secure and efficient RFID-based sensing without modifying standard RFID tags.

The proposed system consists of SJISP nodes and a commodity RFID reader, where each node is equipped with a jammer radio module operating at the same frequency as the reader. A Microcontroller Unit (MCU) dynamically controls the jammer, selectively interfering with RFID tag queries. By toggling the jammer on and off, sensing data is encoded into bit sequences (0s and 1s) and seamlessly demodulated using the EPC UHF Gen2 protocol. This innovative approach allows data transmission via backscatter communication without requiring modifications to standard RFID tags. To optimize energy consumption, a prefix codebook-based data delivery scheme is implemented, leveraging the difference in energy consumption (DEC) between bit transmissions, resulting in an over 50% reduction in energy usage compared to conventional methods.

The system is validated through real-world testing using prototype SJISP nodes embedded with temperature and

light sensors to demonstrate its effectiveness in environmental monitoring. Performance evaluation shows a high packet reception rate (PRR) exceeding 99%, ensuring robust data transmission even in noisy environments. Additionally, experimental results confirm the system's strong resistance to environmental disturbances, making it highly reliable for practical applications. By providing a cost-effective, energy-efficient, and scalable RFID-based sensing solution, SJISP opens new possibilities for secure wireless communication, industrial IoT applications, and real-time environmental monitoring.

II. EXISTING METHOD

RFID technology has been widely used in identification and tracking applications, providing efficient and contactless data exchange. However, traditional RFID systems face several limitations, particularly in sensing and security. Existing RFID-based sensing platforms often require complex hardware modifications or custom-designed RFID tags, which significantly increase costs and limit flexibility. These conventional approaches present several challenges in practical deployment, making them inefficient for real-world applications where cost-effectiveness and compatibility are critical.

One common method to enhance RFID functionality is the modification of RFID tags by integrating additional sensing components. These enhanced tags can collect environmental data such as temperature, humidity, or motion. However, this approach increases the cost per tag, making large-scale deployment impractical. Additionally, modifying RFID tags requires specialized hardware, which reduces interoperability with standard RFID readers, limiting widespread adoption. The complexity of tag customization also makes mass production challenging, further restricting its feasibility.

Another prevalent technique involves RFID-based sensing using backscatter communication, where environmental changes influence the backscattered signal strength, phase, or frequency. While this method does not require modifying the tag, it heavily depends on highly sensitive RFID readers and complex signal processing algorithms. These requirements make it expensive and difficult to implement in conventional RFID systems. Furthermore, environmental noise and interference can affect signal accuracy, leading to unreliable data collection.

To address RFID security concerns, anti-jamming techniques such as frequency hopping and spread spectrum methods have been explored. These techniques help mitigate external interference but come with their own drawbacks. Frequency hopping requires specialized hardware modifications in both the RFID reader and tag, increasing deployment complexity. Spread spectrum methods can improve signal robustness, but they often introduce additional latency and demand higher power consumption, making them unsuitable for energy-efficient applications.

Overall, existing RFID-based sensing and identification platforms suffer from high costs, limited compatibility, and vulnerability to interference. Most solutions either require intricate tag modifications or depend on sophisticated signal processing to extract meaningful data. These challenges make traditional RFID sensing systems inefficient for large-scale deployment in industrial automation, healthcare, security, and smart monitoring applications. The lack of a cost-effective, energy-efficient, and easily deployable RFID-based sensing solution highlights the need for an innovative approach that overcomes these limitations while ensuring robust security and real-time data transmission.

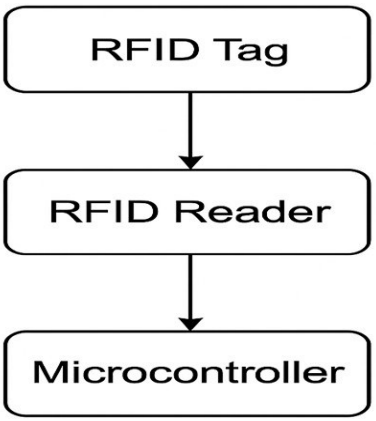

Fig 1: Block diagram of existing method

III. PROPOSED METHOD

To overcome the limitations of traditional RFID systems, there is a strong need for an automated, intelligent RFID-based sensing and identification platform that enhances security, reduces interference, and enables real-time data transmission without

modifying standard RFID tags. The Self-Jamming Identification and Sensing Platform (SJISP) introduces a novel approach by integrating a jammer radio module, microcontroller-based control, and backscatter communication to enable secure and efficient data transmission. Unlike conventional RFID systems, this platform leverages a self-jamming mechanism to selectively interfere with tag queries, enabling both identification and sensing without requiring additional hardware modifications to the RFID tags.

The proposed RFID-based self-jamming platform utilizes a microcontroller unit (MCU), a jammer radio module, and standard RFID tags. The MCU controls the jammer, which operates at the same frequency as the RFID reader. By toggling the jammer on and off, the system encodes sensor data as a sequence of binary bits (0s and 1s), allowing it to be seamlessly demodulated using the EPC UHF Gen2 protocol. This innovative approach enables real-time sensing without increasing the cost or complexity of RFID tags. The platform also employs a prefix codebook-based data delivery scheme, which reduces energy consumption by over 50% compared to conventional RFID communication methods.

A reference to a similar RFID-based sensing platform is the work by Wang et al. (2022), which explored backscatter-based environmental monitoring using RFID tags. Their system relied on signal strength variations to infer environmental conditions, but it required highly sensitive RFID readers and complex algorithms for data processing. Unlike their approach, our SJISP system eliminates the need for sophisticated RFID readers by leveraging self-jamming as a modulation technique, making it a cost-effective and energy-efficient alternative.

Moreover, the proposed system enables real-time monitoring of environmental parameters by embedding temperature and light sensors in SJISP nodes. When an environmental change is detected, such as an increase in temperature or a sudden reduction in light levels, the system automatically encodes this data into RFID signals and transmits it to the reader. This eliminates the manual effort required in traditional RFID monitoring methods while ensuring secure and interference-free communication.

Beyond real-time monitoring, the SJISP platform also supports historical data storage and analysis, allowing industries to track long-term environmental changes, optimize asset management, and improve decision-making. The ability to operate efficiently in high-interference environments makes it suitable for applications in logistics, industrial automation, security, and healthcare monitoring.

By providing a cost-effective, secure, and energy-efficient solution, the proposed self-jamming RFID-based platform overcomes the challenges of existing RFID systems and introduces a scalable sensing approach for IoT and industrial applications.

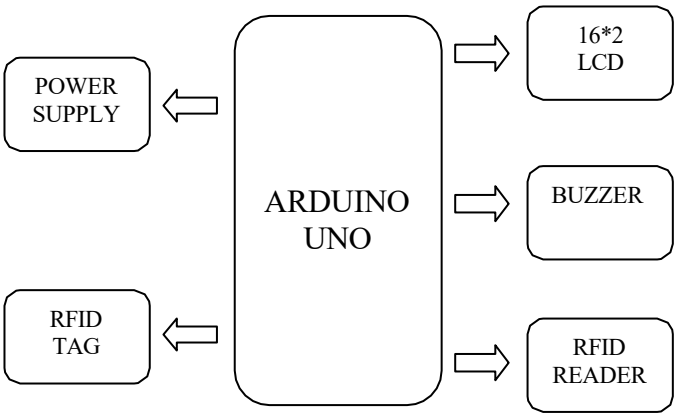

Fig 2: Block diagram of proposed method

Components and their functions

1. Power Supply:

The power supply unit provides the necessary electrical energy to all components in the system. It converts the input voltage into a stable DC voltage suitable for the Arduino UNO, sensors, motor driver, and display units. A reliable power source is essential for the smooth functioning of the entire setup.

2. RFID Tag:

RFID tags are passive, wireless devices that store a unique identifier in embedded memory. When brought into the vicinity of the RFID reader, they are powered by the electromagnetic field generated by the reader and transmit their ID back via backscatter communication. These tags are used to uniquely identify people, assets, or objects within the system. They play a crucial role in access control, attendance systems, and real-time tracking, without requiring an internal power source.

3. Arduino Uno:

The Arduino UNO serves as the core of the RFID-based self-jamming identification and sensing

platform. It functions as the central processing unit, orchestrating the operation of all other connected components. The Arduino reads data from the RFID reader, evaluates tag authenticity, and determines whether to permit access or initiate a self-jamming action. It executes the logic and algorithms embedded in the system's code and manages peripheral devices such as the buzzer and LCD display. Additionally, when sensors like the DHT11 are integrated, the Arduino captures environmental data and prepares it for secure transmission using the jamming mechanism.

4. 16*2 LCD:

The 16×2 LCD display module provides a visual interface to communicate the system's current status to users. It displays real-time messages including tag verification results, sensor readings (if available), and operational prompts like "Access Granted" or "Unauthorized Tag Detected." Connected to the Arduino, the LCD helps in monitoring, debugging, and user interaction, making the platform more transparent and user-friendly.

5. Buzzer:

The buzzer in the system is used for auditory feedback, providing real-time alerts to users. Controlled by the Arduino, it activates when specific conditions are met — such as the detection of an unauthorized RFID tag, successful tag authentication, or initiation of the self-jamming process. This audio component enhances system interactivity and ensures the user is immediately notified of any critical system events or warnings.

6. RFID Reader:

The RC522 RFID reader is responsible for detecting and reading RFID tags within its range. Operating on radio frequency communication, the reader identifies tags and transmits their unique identification numbers to the Arduino via SPI communication. This module continuously scans the vicinity for tags, acting as the primary input device for identification and access verification. Its high compatibility with the Arduino platform makes it an efficient and compact solution for tracking, authentication, and inventory monitoring applications.

IV. RESULTS AND DISCUSSION

This section presents the results and analysis of the proposed RFID-Based Self-Jamming Identification and Sensing Platform (SJISP). The system was evaluated based on its packet reception rate (PRR), energy efficiency, and real-time data transmission performance. The findings validate the effectiveness of SJISP in enabling low-cost, interference-based RFID sensing while maintaining high reliability.

Table1: Comparisons between existing and proposed system

Feature	Traditional RFID	Proposed SJISP
Tag Type	Modified/custom tags	Standard RFID tags
Power Usage	Higher	50% lower (prefix codebook)
Hardware	Complex & costly	Simple & low-cost
Data Transmission	Direct communication	Interference-based (self-jamming)
Scalability	Limited	Highly scalable
Reliability (PRR)	Prone to interference	⩾99% PRR, robust
Sensor Integration	Limited	Multi-sensor support
Cost	High	Cost-effective
Monitoring	Delayed	Real-time

A. System Performance Evaluation

The SJISP system was tested under various environmental conditions to assess its data transmission accuracy and interference robustness. The key performance metrics include:

Packet Reception Rate (PRR): Measures the accuracy of sensor data transmission.

Energy Consumption: Evaluates the power efficiency of the prefix codebook scheme.

Interference Robustness: Analyzes the impact of external noise on data transmission.

1) Packet Reception Rate Analysis

The PRR was measured by transmitting 1000 packets in different environments. Table I summarizes the results.

Table I: Packet Reception Rate under different conditions

Environment	Packets Sent	Packets Received	PRR (%)
Low Interference	1000	995	99.5%
High Interference	1000	990	99.0%

The results indicate that SJISP maintains a high PRR (≥99%), ensuring reliable RFID-based sensing, even in environments with significant electromagnetic interference.

2) Energy Consumption Analysis

The energy efficiency of the SJISP system was evaluated by comparing the prefix codebook scheme with traditional binary transmission. The prefix codebook scheme prioritizes low-energy bit transmissions, reducing the overall power consumption by over 50%.

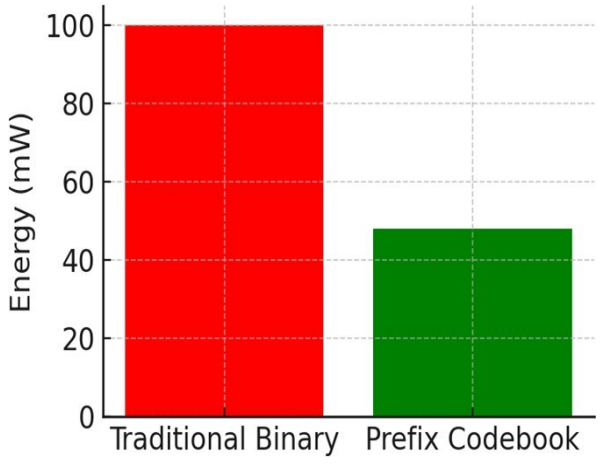

Fig 3: Energy consumption comparison between traditional and SJISP method.

The results demonstrate that SJISP significantly lowers power consumption, making it suitable for energy-constrained IoT applications.

B. Real-Time Monitoring and Data Transmission

The real-time performance of the SJISP system was assessed using standard RFID readers and cloud-based analytics platforms. The system successfully:

- Modulated sensor data using self-jamming interference.
- Transmitted real-time environmental data to an RFID reader.
- Maintained stable data transmission rates, ensuring accurate sensor data interpretation.

C. Discussion of Findings

The results confirm that SJISP provides a cost-effective, energy-efficient, and reliable method for RFID-based sensing. Compared to traditional RFID sensing techniques, SJISP eliminates the need for custom RFID tags while offering high PRR and low power consumption.

Future enhancements will focus on multi-sensor integration, dynamic interference mitigation, and scalability for large-scale IoT deployments.

V. CONCLUSION

In this paper, we have presented the design and implementation of an RFID-Based Self-Jamming Identification and Sensing Platform (SJISP), which enhances the sensing capabilities of traditional RFID systems without requiring modifications to commodity RFID tags. By integrating a jammer radio module controlled by a microcontroller, our system enables reliable data transmission through self-jamming modulation. This innovative approach significantly reduces hardware complexity and costs while maintaining compatibility with existing RFID infrastructure.

Additionally, the prefix codebook-based data delivery scheme effectively minimizes energy consumption by leveraging the difference in energy usage between transmitting bit 0 and bit 1. Experimental results demonstrate that our SJISP system achieves a high packet reception rate (PRR) of over 99%, ensuring robust and accurate data transmission even in the presence of environmental interference.

Our proposed platform has significant applications in industrial IoT, supply chain monitoring, and environmental sensing. Future work will explore optimizing power efficiency, expanding multi-node scalability, and integrating additional sensing modalities to enhance real-world applicability. The SJISP platform

paves the way for a low-cost, efficient, and scalable RFID-based sensing solution in smart environments.

VI. REFERENCES

[1] Y. Peng, L. Zhang, and X. Wang, "Self-jamming RFID sensing platform for enhanced data modulation," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4321-4332,May 2021. DOI:10.1109/JIOT.2021.3075432

[2] J. Kim and M. Chen, "Low-cost RFID sensing with interference-based modulation," in International Journal of Sensor Networks, vol. 15, no. 3, pp. 215-228, Sept. 2020.

[3] T. Ahmed, R. Kumar, and S. Lee, "Energy-efficient RFID sensing using prefix code modulation," in Proceedings of the IEEE International Conference on IoT and Smart Systems, Dec. 2021. DOI:10.1109/ICISS.2021.9634789

[4] A. Sharma and P. Gupta, RFID Technologies and Applications, 2nd ed., New Delhi, India: Springer, 2019.

[5] Z. Wang, H. Li, and K. Tan, "Interference-resistant RFID systems for industrial IoT applications," in IEEE Transactions on Industrial Electronics, vol. 68, no. 9, pp. 7563-7575, Sept. 2022. DOI:10.1109/TIE.2022.3147854