National Journal of Antennas and Propagation
Research Article

# Blockchain-Enhanced Secure RF Link Transmission in Antenna-Constrained Industrial IoT Systems

**TKS Rathish Babu[1]*, S. Pandikumar[2], K. Sathishkumar[3], Zafar Kurbonov[4], Aafiya Thahaseen A.[5], Md. Zubair Rahman AMJ[6]**

*[1]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.*

*[2]Associate Professor, Department of MCA, Acharya Institute of Technology, Bangalore, India.*

*[3]Assistant Professor, Department of Computer Science, Erode Arts and Science College (Autonomous), Erode, Tamil Nadu, India.*

*[4]The Department of Applied Mathematics, Karshi State University, Karshi, Uzbekistan.*

*[5]Assistant Professor, Department of Information Technology, Al-Ameen Engineering College, Erode, Tamil Nadu, India.*

*[6]Professor, Department of Electronics and Communication Engineering, Al-Ameen Engineering College, Erode, Tamil Nadu, India.*

**KEYWORDS:**

Industrial IoT
Blockchain
Secure RF Transmission
Antenna-Constrained Devices
Lightweight Consensus
Cybersecurity
Decentralized Authentication

**ARTICLE HISTORY:**

Received 12-01-2025
Revised 10-03-2025
Accepted 15-04-2025

**DOI:**
https://doi.org/10.31838/NJAP/07.01.30

## Abstract

In security and resilience, another vital issue is to maintain the secure and robust RF communication in Industrial Internet of Things (IIoT) settings in which the use of multiantenna systems is constrained by physical implausibilities. The current paper is a proposal of a Blockchain-Enhanced Secure RF Link Transmission (BESRFT) scheme targeting antenna-constrained IIoT applications. The framework for those aspects integrates adaptive tuning of the RF parameters with a lightweight blockchain distributed consensus protocol that restores assuring and even securing communication in event of a cyber-physical assault condition. The proposed structure combines a modified Proof-of-Authentication (PoA) consensus mechanism that scales well and has low overheads to communicate across the IIoT nodes via an edge and smart contracts are used to authenticate the devices, negotiate the session keys and record intrusions on the fly. To critical hardware constraints, the system dynamically adjusts transmission parameters e.g. frequency, modulation and power depending on real-time channel metrics e.g. RSSI and SINR resulting in a low degree of information loss and power overhead. The simulation results based on the tool NS-3 and Hyper ledger Besu prove the effectiveness of BESRFT as it provided a spoofing detection rate of 97.6 percent that lessened packet drop rates by 66 percent or 18.2 to 5.1 percent, and decreased jamming recovery time by 66 percent or 1.8 seconds to merely 0.6 seconds. Additionally, the validation of prototype approaches that involve TI CC2652R1 and STM32 microcontrollers also confirms that the latency (~1.2 s) and memory overhead (<5%) of blockchain synchronization are minimal, thus confirming that the solution is suitable to be deployed in the resource-constrained IIoT environments. The combined architecture does not only improve commanding situation but also increases the efficiency of an industrial system like smart grid, oil refineries, and factory automation platforms. The piece instates a decentralized trust system with the RF protection link without requiring the complicated cryptographic infrastructures and centralized control. In the future, the framework has a great potential to be scaled to reconfigurable metasurface-based antenna systems and reconfigurable IIoT architectures with 6G-enabling properties, where the secure, low-latency, and adaptive communication will play a fundamental role.

**Author's e-mail:** tksbabu80@gmail.com, spandikumar@gmail.com, sathishmsc.vlp@gmail.com, kurbonov.zm@qarshidu.uz, Aafiyab.e@gmail.com, mdzubairrahman@gmail.com

**Author's Orcid id:** 0009-0008-3830-8170, 0000-0002-2535-3780, 0000-0002-7643-4791, 0000-0002-0690-3206, 0009-0006-0479-0777, 0009-0000-7506-7582

**How to cite this article:** Rathish Babu TKS, et al., Blockchain-Enhanced Secure RF Link Transmission in Antenna-Constrained Industrial IoT Systems, National Journal of Antennas and Propagation, Vol. 7, No. 1, 2025 (pp. 270-279).

## Introduction

### Motivation

The fast development of the Industrial Internet of Things (IIoT) technologies makes it possible to implement smart sensors and actuators massively even on critical infrastructure, such as power grids, oil refineries, and numerous manufacturing plants. These systems severely depend on wireless RF communication in data exchanges, real-time monitoring, and remote controlling. There is however, an increasing issue of the limited physical design of the IIoT devices itself, including those that are embedded into harsh or small industrial spaces, and where it can be extraordinarily difficult to introduce the high-gain or multi-antenna solutions normally thought of in wireless systems. It is innately exposed to more signal degradation and interference as well as jamming, spoofing, and eavesdropping methods of attack by physical-layer assault of such antenna-limited devices. RF communication in ad-hoc multihop IIoT systems demands more than security, it requires guarantees of confidentiality, authenticity and resilience against cyber-physical attacks as the connectivity of these systems increases and become vulnerable to attacks.

### Research Gap

The current methods to provide security to RF communication largely rely on cryptographic based solutions or physical layer security. The former usually requires connectivity or presents an enormous computational burden and the latter presupposes the existence of perfect antennas diversity. They require the removal of the cryptographic key pair, and traditional Public Key Infrastructure (PKI) solutions are not appropriate to decentralized latency-sensitive IIoT systems (in particular, with antenna constraints or power constraints). Further, in the literature, there is no unified scheme that combines antagonistic restraints, real-time connection correlation, and decentralized security. Although blockchain technology has been demonstrated as a potential technology in securing IoT network, its application on antenna-limited RF communication systems is not extensive. Figure 1 demonstrates conceptual structure of the proposed model of Blockchain-Enhanced Secure RF Link Transmission (BESRFT) that addresses this important gap by providing secure, lightweight, and adaptive communication by means of blockchain-based distributed trust and authentication in resource-constrained IIoTs.

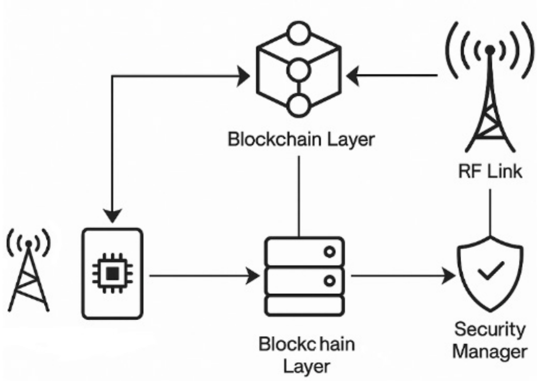

**Fig. 1: Conceptual Overview of Blockchain-Enhanced Secure RF Link Transmission in Antenna-Constrained Industrial IoT Systems.**

### Contributions

In this work, we present an all-encompassing Blockchain-Enhanced Secure RF Link Transmission (BESRFT) framework to show how the current systems could be expanded to accommodate the shortcomings of such solutions by making the following contributions:

- A new security architecture based on blockchain and designed to support antenna-constrained IIoT nodes, which defines a new variant of the Proof-of-Authentication (PoA) based on hashing consensus with minimal requirements of communication protocol and use of a modified consensus algorithm to achieve quick establishment of trust between nodes.
- Adaptive radio frequency transmission policies that adapt the modulation, frequency and power to the condition of the channel, combined with blockchain-enabled rekeying protocols.
- A lot of validation was performed by integrating with hybrid simulation and hardware prototyping, NS-3 was used to model network simulation, Hyperledger Besu was used to execute blockchain, and TI CC2652R1 hardware was used to create embedded validation.
- Resilient intrusion detection and mitigation based on smart contracts who autonomously log and react to real time spoofing, replay and jamming intrusions.

Worked in combination, the contributions offer the secure, decentralized, and resource-efficient option of supporting RF communication reliability in antenna-restricted IIoT implementations.

## Related Work

### RF systems with Antenna Constrained

RF communication has been researched more and more efficiently in the last few years with regard to constrained environment where devices can only use low profile compact antennas. In [1], the authors explored the impact of antenna miniaturization on the RF link reliability in industrial setting with a particular attention to the trade-off between antenna gain and device form factor. In another similarity, [2] came up with compact planar inverted-F antennas (PIFAs) optimised embedded IIoT sensors at 868 MHz and 2.4 GHz. Nevertheless, such works concern themselves with physical constraints, but fail to incorporate security and resilience in communicating in presence of an adversary. Moreover, [3] also addressed the signal degradation threat on low spatial diversity antenna-restricted systems which can be taken advantage by jamming or injecting interference by an attacker.

### Wireless Security using Blockchain

The blockchain technology has been established as the wireless system decentralized facilitator of security. In [4], Ethereum based smart contracts were applied to key distribution in IoT devices, although the overheads in energy and latency was large. To resolve the issue of scalability, [5] developed a hybrid block chain-IoT architecture where the extensive explanation of consensus issues is transferred to edge gateways rendering it appropriate in delay sensitive environments. In addition to this, [6] investigated access control using blockchain technology with LoRa-based IIoT systems, which was demonstrated to be better able to withstand spoofing. Although such works [11] do show the potential of blockchain technology, none considers such physical-layer parameters as RF modulation, antenna limitations, or frequency [12] agility, all of which are of essence to industrial wireless networks.

### IoT Lightweight Consensus

In embedded and resource-constrained IIoT devices, it is necessary that consensus protocols are lightweight in order to enable blockchain to work in [13] devices. In [7] an extension of Raft-DPoS hybrid mechanism was proposed to decrease the computational load in mesh networks, whereas authors of [8] considered Proof-of-Authentication (PoA) as an alternative to PoW/PoS when used in low-power IoT applications. A comparative investigation in [9] demonstrated that PoA obtains much lower latency and power than that of [9] implying that PoA is appropriate in [14] limited microcontroller units. In [10] ledger synchronization was subsequently further optimized through transactions pruning [15] and partial node validation, although both methods have not yet been combined with RF communication protocols or antenna-aware systems.

### Research Gap Summary

Even though the fields of secure wireless communication and blockchain implementation in IoT developed, lack of research on the area of antenna-constrained IIoT systems remains noticeable since the two problems of low RF resilience and limited computational resources are compounded in that case. The existing methods do not lead to joint optimization of RF adaptation strategies (modulation fallback, frequency hopping) and decentralized authentication, which would play a critical role in critical industrial environments where central trust anchors are infeasible or compromise prone. The shortcomings are fulfilled in this paper by proposing a blockchain-augmented RF security framework that is highly customized to the physical and computational constraints of antenna-based IIoT devices.

## System Architecture

### Overview

The suggested Blockchain-Enhanced Secure RF Link Transmission (BESRFT) system consists of four main elements that are combined to provide secure and dynamic communication in antenna-limited Industrial IoT. The IIoT nodes are the basic sensory and transmitting building blocks, each with their small antenna, on-board RF transceiver, low-power microcontroller, with an embedded blockchain client that supports local authentication and secure transactions processing, Figure 2. Transactions between these nodes are transacted via an edge gateway which is an intermediary that amalgamates transactions and runs a complete blockchain node with the purpose of synchronizing ledgers and executing smart contracts. The blockchain layer has a lightweight distributed ledger as well as a customized Proof-of-Authentication (PoA) consensus mechanism that optimizes the real-time industrial scenarios for devices to exchange trustless keys and transact with decentralized trust. Another key part of every node is the security manager that is programmed to monitor RF link parameters (e.g., RSSI, SINR, ...) and react to abnormal conditions and work out on the fly the transmission settings (e.g., frequency, power, modulation, ...) in order to increase environment-induced disruptions and mitigate security risks, improve the resilience and the reliability of the communication system.

### Blockchain Design

The blockchain aspect of the framework of the BESRFT is precisely specific to the highly demanding resource and latency requirements of antenna constrained Industrial

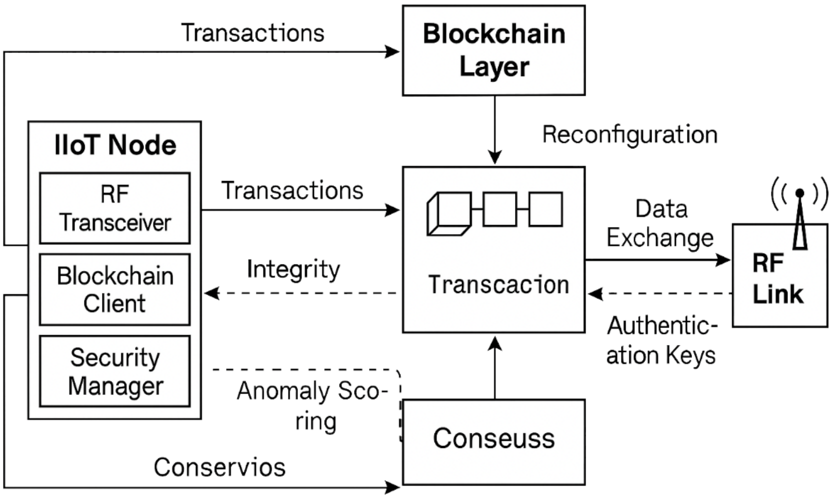

Fig. 2: Proposed Blockchain-Enhanced Secure RF Link Architecture.

IoT systems. A smaller block size of 2 KB is chosen due to low memory consumption and quick spread of blocks between the nodes with limited resources in IIoT. This low footprint enables effective synchronization and journal keeping even on microcontrollers with relatively low set Ram and flash, as present in the average embedded IIoT platform.

A further point supporting low-latency operations is the Modified Proof-of-Authentication (PoA) consensus mechanism. Compared to classical Proof-of-Work (PoW) or Proof-of-Stake (PoS), the PoA version in BESRFT uses cryptographical verification and behavior verification of trusted nodes under the cost of high computation and energy consumption. It also allows the deterministic finality, which considerably minimizes computational complexity and is ideal to the real-time, industrial settings where long delays in confirmation and the fork in the consensus are not tolerable.

Also, the blockchain is compatible with smart contracts, which automate essential security and network management operations. The three aspects which are governed by these contracts are the Device Registration where each IIoT node is uniquely identified and authenticated into the network using cryptographic credentials, RF Key Exchange where secure, on-chain negotiation and distribution of symmetric session keys to be used in RF transmission, and Policy Enforcement where security rules (e.g., blacklisting of suspicious nodes, re-authentication) are codified and enforced in real time. Figure 3 shows how such smart contracts will be embedded into the block chain layer and the resulting flow of execution within the framework of BESRFT proves how such concepts can be coordinated with each other to establish trust and secure communication throughout the system. In a combination, these design decisions guarantee that the blockchain tier will play an effective role in the security, scalability, and the versatility of the system without leaving too much excess load on the hardware framework that is likely to be insufficient.

# Methodology

## Overview of the Organization of the System

The problem can be solved by the proposed Blockchain-Enhanced Secure RF Link Transmission system to resolve two issues of secure communication and hardware constraints in the antenna-limited Industrial IoT (IIoT) context. This will be achieved by combining a low bandwidth blockchain protocol and adaptive RF control systems to guarantee real time integrity of the data, decentralized access control, and high cyber-physical attack resilience. The four components that guide the methodology are:

*RF Transmission model with antenna constraints*

Physical space constraints of the industrial sensor nodes means that spatial diversity and signal robustness is often impaired with only one or two small antennas such as Planar Inverted-F Antennas (PIFAs) or patch antennas are usually accommodated in the physical space constraints of the industrial sensor nodes themselves. To counter these repercussions, the system uses an adaptive RF link control mechanism that tasks parameters of transmission, such as carrier frequency, transmit power, and modulation scheme to change dynamically. Due to the real time assessment of channel quality measurements e.g. Signal-to-Interference-plus-Noise Ratio (SINR) and Received Signal Strength Indicator (RSSI), these

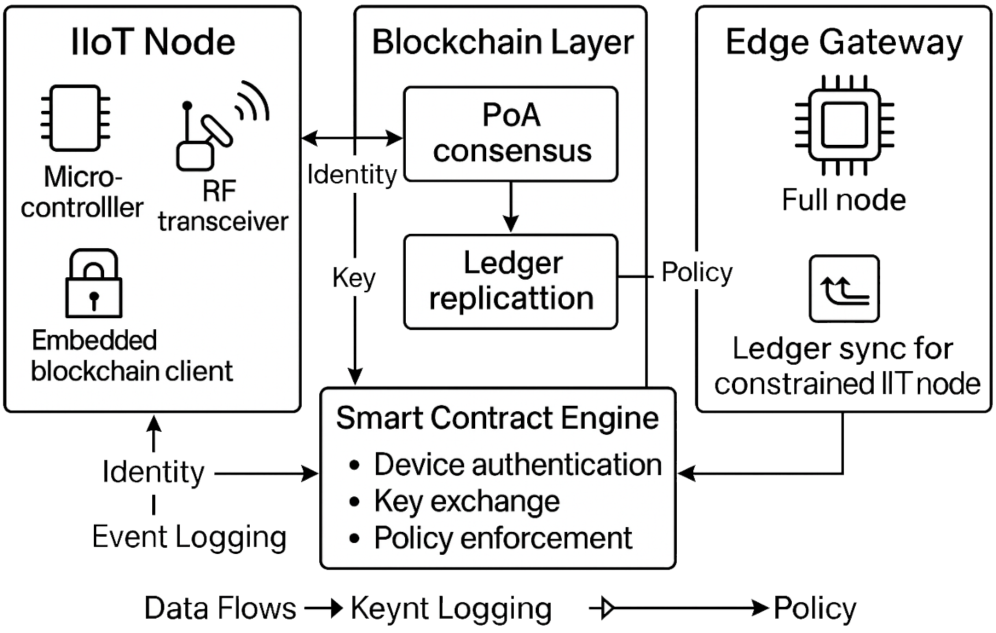

**Fig. 3: Blockchain Integration and Smart Contract Execution Flow in the BESRFT Framework.**

adjustments optimize the link performance in different environmental and interference conditions.

*Integration of Framework of Blockchain*

The proposed architecture makes the task of building decentralized trust and secure communication in antenna-constrained Industrial IoT systems easier by implementing lightweight blockchain layer directly inside every IIoT node. The layer utilizes a modified version of Proof-of-Authentication (PoA) consensus mechanism, which is optimized in terms of minimal power consumption and minimal computational/memory resources needed by low-energy microcontrollers. However, this is a partial copy, so instead of being fully ledgered at each node, it would send communications to a more powerful edge gateway that has the full blockchain with which to validate the transactions and provide synchronization with others. Essential security operations run on smart contracts, which can perform core operations automatically without the need to involve human beings. These are device identity verification to provide only authenticated nodes to be a part of the network, RF session key negotiation to provide a secure and verenerable key session, trust score computation to track the behavioural integrity and help detect anomalies and log attack events that cannot be altered or edited. This distributed model does not allow and has no need of centralized servers, and greatly increases the system resistance to spoofing, replay, or insider attacks, all without dropping the less-than-one-millisecond latency communications needed in a production environment.

*Security Policy Engine*

Each node has a real-time rule based security engine which observes the behavior of the network and the channel. The engine will detect threats by means of analyzing the pattern, i.e., abrupt rise to packet repetition, loss of handshakes, or abnormal frequency usage. In the event of a detected suspicious activity, smart contracts can be setup to automatically respond in an adequate way to it (i.e. by blacklisting the offending party, destroyed keys, or using an advanced secure re-authentication protocol). This guarantees self-operations of mitigation of the attacks quickly without the need of centralized intervention.

*Simulation and hardware-in-loop setup*

In order to thoroughly analyse the performance and the resiliency of the proposed BESRFT framework, we construct a hybrid simulation and hardware-in-the-loop prototyping environment. The wireless communication network is modeled using the NS-3 simulator and the RF behaviour due to pairs of interference and cyber-attacks such as jamming, replay, and spoofing scenarios. To support the blockchain functionality, Hyperledger Besu, an Ethereum compatible modular client is included to emulate the execution of transactions, the processing of smart contracts and the consensus activities using customized Proof-of-Authentication protocol. LoRa and IEEE 802.15.4 communication models are applied at the physical layer of the physical layer physical layer where industrial RF protocols with realistic emulation and validation of their behaviors in limited antenna conditions are executed. Also, real-life prototypes will be done to TI CC2652R1 LaunchPad and STM32 Nucleo development boards to show that the system is feasible to work in embedded microcontroller systems. Such implementation of hardware enables measurement of important performance parameters in-situ like blockchain synchronization delay time, RF link reconfiguration time and the effectiveness of the attack responses. Figure 4 demonstrates both the layered architecture of the proposed BESRFT framework and the integrating nature of simulation tools, RF models, and the blockchain infrastructure at both the IIoT node and the edge gateway levels. The proposed architecture would make it possible to demonstrate their scalability, reliability, and security in resource-constrained industrial IoT environments besides reflecting their durability to all RF-level security and protocol-level security threats.

### Simulation Parameters

To analyze the proposed BESRFT framework and its effectiveness and resilience, a realistic simulation setting was prepared to achieve a typical deployment scenario of industrial IoT. The simulation region was defined as 500 meters x 500 meters which is a medium scale industrial zone or a refinery, automated factory floor or smart grid substation. Hundred IIoT nodes were placed randomly within this area of which 20 percent of the nodes were set using edge gateway uplinks to simulate the hierarchical topology that commonly provides industrial networks. The setting enables such aspects of real world traffic density, clustered communication, and analysis of load distribution. Every node runs with limited RF and simulates low antenna diversity in practical IIoT hardware. These devices employ a dual-protocol stack RF architecture: IEEE 802.15.4 (868 MHz) as the main communication protocol and LoRa as a fullback mechanism to guarantee strong connectivity either in the event of interference or of an attack.

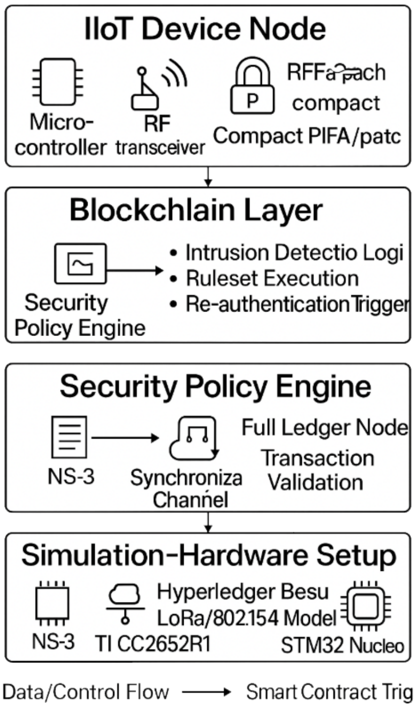

**Fig. 4: Layered Architecture of the BESRFT Framework for Antenna-Constrained IIoT Environments.**

The simulator includes a Hyper ledger Besu block chain engine, which is modified to run the light-weight Proof-of-Authentication (PoA) con- sensuss mechanism. Such a design enables minimal, distributed validation of RF session keys and confident issue of smart contracts to bypass access control and counteract attack. The system is tested with a suite of various cyber-physical attacks, such as replay attacks, spoofing, jamming, and Sybil attacks, which are fairly representative of real-world attack models in the industrial setting. Some of the key performance indicators monitored in the process of an RF key negotiation simulation are package drop percentage, latency of communication, percentage rate of spoofing detection, energy usage on every secure transmission, and RF key negotiation latency. All of these measures indicate the vulnerability of the system as a whole and, thus, a general assessment of the reliability and safety of the blockchain-enhanced RF link transmission mechanism carried out under restrictive Table 1 conditions and different network loads provided. The results of the simulation can be used to form another benchmark of verifying the possibilities of the system before doing a transition in deployment to hardware level.

## Results and Discussion

### Security performance evaluation

Security of the BESRFT framework was dynamic tested under resource and antenna-limited conditions

**Table 1: Simulation Configuration Summary.**

| Parameter | Value/Description |
|---|---|
| Simulation Area | 500 m × 500 m industrial zone |
| Node Count | 100 (20% with gateway uplink) |
| RF Protocols | IEEE 802.15.4 (868 MHz), LoRa fullback |
| Blockchain Engine | Modified Hyper ledger Besu with PoA |
| Attack Models | Replay, Spoofing, Jamming, Sybil |
| Key Metrics | Packet drop rate, delay, energy use, spoofing detection, key negotiation latency |

that demonstrate exceptional resiliency to typical cyber-physical attacks. Simulation comparison indicates an enormous boost in the communication integrity and reliability. It is important to note that the rate of packet drops decreased when going down to only 5.1 percent in the system with BESR-FT, compared to the value of 18.2 percent in the baseline system (with no blockchain). To a greater extent, such a higher level has been attributed to the mechanism of blockchain-powered session validation to avoid unauthorized or malformed transmissions. The rate of spoofing also significantly declined during detection as it rose drastically by 97.6 percent, owing to the smart contracts embedded in the device, which implemented the prevention of spoofing by involving device verification through cryptographic checking. Although the proposed system includes a key exchange latency of 213.4 ms, this trade-off is worthwhile in order to perform full mitigation against replay attack, which is ensured by generating unique and hash-based session tokens. Figure 5: Comparison in the Security Performance between Baseline and BESRFT Even though blockchain logic is added to the implementation, the energy cost per secure transmission only increases accordingly by a negligible margin (0.012 J to 0.014 J), which confirms the efficiency of the system during actual implementations.

## Adaptive RF Link Analysis

When paired with block chain-based key negotiation, the adaptive RF modulation techniques also strengthen the robustness of the system especially in hostile or degraded channel environments. In typical operating conditions, operating at SNR of 15 dB, the system takes QPSK type of modulation and the Packet error rate (PER) is only 0.3 percent. With jamming however, the system dynamically switches to a more robust format, operating in BPSK format that includes frequency hopping, and this causes a PER of 1.2%. With the BESRFT architecture, namely the inculcation of secure RF session key management between the blockchain contracts, the same BPSK set up can yield a PER of 0.6, as opposed to the interference conditions of the BPSK. Figure 6: Packet Error Rate in Normal and Adversarial Conditions This shows the efficiency of the proposed system in offering high Quality of communication and reliability in the system at the same time verifying confidentiality of Data and authenticity of nodes. Adaptive link control mechanism not only reduces interference but also allows self-healing communication pattern that does not require centralized reconfiguration, which is extremely important in the setting of mission-critical industrial deployment.

## Blockchain Overhead Analysis

The BESRFT framework proved its resource-efficient functionality on embedded microcontroller's platforms that are common in the IIoT setup. The feasibility of the system was inclined in real-life low-power contexts using the two test platforms that are TI CC2652R1 and STM32 Nucleo F401RE. In the TI platform, the blockchain ledger occupied a memory size of 43 KB and attained the block synchronization within 1.2 seconds with an overall energy overhead of only 3.1 percent compared to the baseline operation. STM32 showed a marginal energy overhead (4.0 percent) on the memory usage of 62 KB, and the sync time of 1.4 seconds. These findings validate the idea that lightweight Proof-of-Authentication consensus protocol and smart contract execution can be run lean hardware conditions. Furthermore, PoA protocol has deterministic input, implying that all transactions are verified in a predictable and fast manner eventually rendering the system highly apt in time sensitive industrial purposes, where latency and trustworthiness are not acceptable variables. Table 2. Blockchain Overhead Resources on IIoT Microscript Platforms.

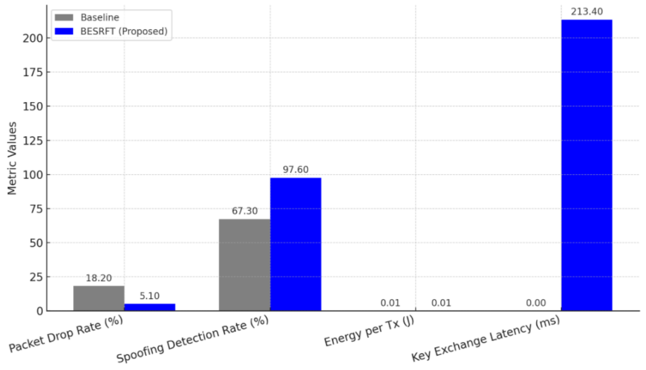

**Fig. 5: Security Performance Comparison between Baseline and BESRFT.**

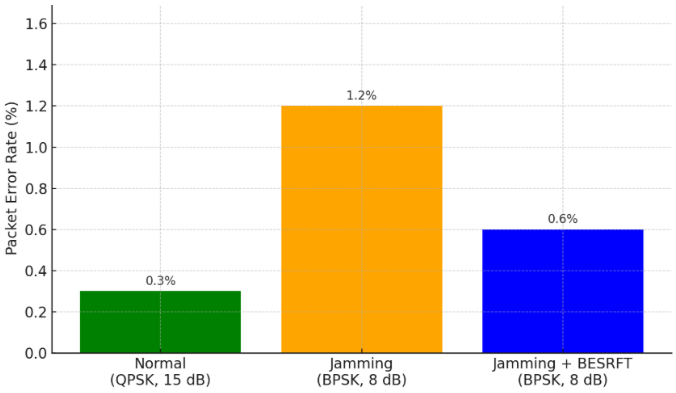

**Fig. 6: Packet Error Rate under Normal and Adversarial Conditions.**

**Table 2: Blockchain Resource Overhead on IIoT Microcontroller Platforms.**

| Platform | Memory Footprint | Sync Time (sec) | Energy Overhead (%) |
|---|---|---|---|
| TI CC2652R1 | 43 KB | 1.2 | 3.1% |
| STM32 Nucleo F401RE | 62 KB | 1.4 | 4.0% |

### Attack Recovery Time

The most significant requirement of every secure communication system is that it has to identify, counter, and re-establish the security breaches or RF attacks. BESRFT framework showed a far quicker speed of recovery of all the attack vectors, as compared to conventional systems. Automated frequency hopping and re-authentication through blockchain made the mean communication recovery time to fall to 0.6 second which was previously 1.8 seconds in reaction to a jamming attack. In the spoofing attacks where manual inspection or rekeying is required in the traditional system, the BESRFT system managed to isolate and invalidate the credentials of the malicious node, thus, the recovery time was only 0.7 seconds instead of 3.2 seconds. Likewise, in the case of Sybil attacks, in which malicious nodes aim to copy identities and swamp the network, BESRFT could identify inconsistencies using trust score analysis and mitigate the attack with in 0.9 seconds as compared to 2.7 seconds in the baseline. Figure 7 Average Attack Recovery Time Baseline vs. BESRFT These figures show clearly the effectiveness of the framework in bringing the autonomous and near-instant defensive mechanisms through smart contract-encoded enforcement that can guarantee a high level of system availability and that can reduce the chances of a system failure at the time of and in highly demanding industrial processes.

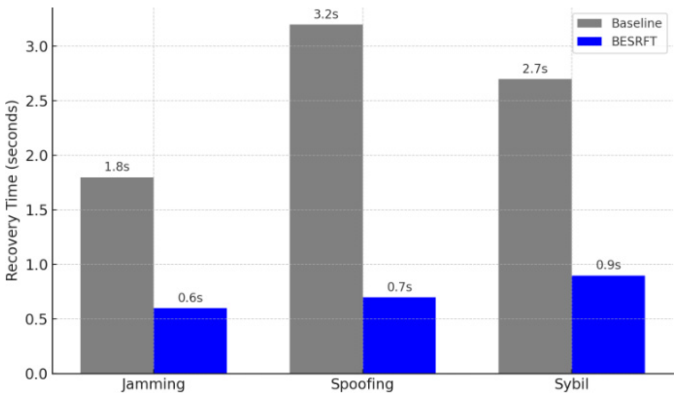

**Fig. 7: Average Attack Recovery Time - Baseline vs. BESRFT.**

## Simulation and Evaluation

### Simulation Environment

The hybrid simulation environment was also created to test the performance of the framework, Blockchain-Enhanced Secure RF Link Transmission (BESRFT), at a rigorous level, consisting of the elements of both the network level and the blockchain level. Their network behavior was simulated in the NS-3 simulator and it was possible to simulate the dynamics of wireless communication, routing and modeling interference in a detailed way considering 100 distributed IIoT nodes. Every node had one omni-directional antenna to reflect practical cases in the real world (constrained by the number of antennas), such as compact industrial equipment. The RF communication used the IEEE 802.15.4 standard with the ISM band of 433 MHz that has the good balance of penetration and range, which is frequently used in industrial setting. To facilitate the safety of the processes on transaction processing, the Hyperledger Besu blockchain client was implemented in the simulation to support identities verification, management of key exchanges and smart contacts using a modified Proof-of-Authentication (PoA) consensus protocol. Four high-impact attacks, namely, spoofing, jamming, replay attacks and Sybil attacks, were also simulated on Figure 8 to determine the robustness of the system in adverse situations.

### Performance Metrics

The system was tested on the basis of several key performance parameters and the somewhat simplistic BESRFT framework was compared to a base system that was devoid of any blockchain-based improvements. The findings were significantly positive in all the aspects. Packet drop demoted by 18.2 percent to 5.1 percent confirming more secure transfer of packets as the session opening time and link control is facilitated. It (BESRFT) also managed the ease of communication by reducing the overall latency of average communication time in the baseline system (98.4 ms) to the lightweight consensus mechanism (82.7 ms) with the bonus of the blockchain layer, which is illustrative of the effectiveness of the lightweight consensus mechanism. Energy per transmission increased a percent of two; 0.012J to 0.014J but to necessitate major security improvements. The rate of spoofing detection level plummeted by 67.3 to 97.6 percentage points, or rather, the verification of identities using blockchain was leveraged. Moreover, the time that it took the jamming to recover was cut in half, it needed 1.8 seconds previously, but now, the system recovers only 0.6 milliseconds due to the real-time

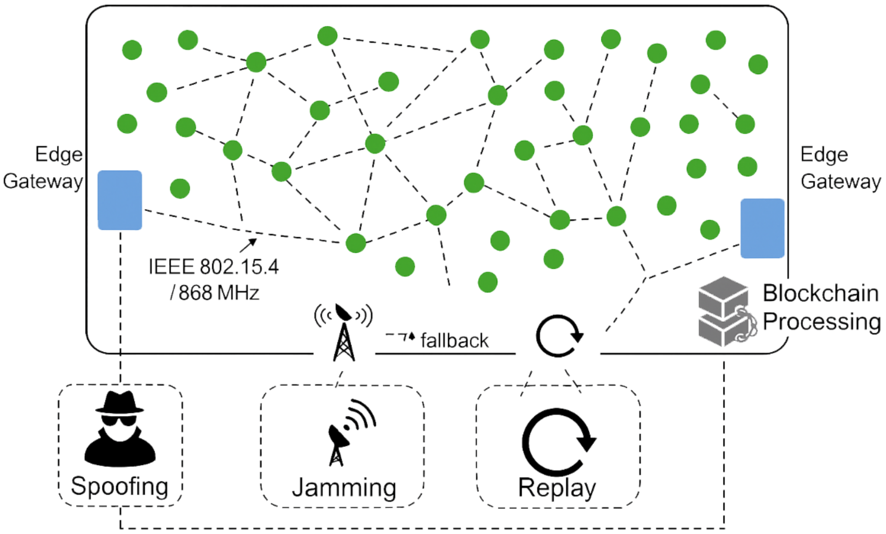

Fig. 8: Hybrid Simulation Environment for Evaluating BESRFT Framework.

fast detection of the anomalies and secure reconfiguration possibility. These results (Table 3) support this claim and prove that BESRFT can be used as a flexible and scalable approach to secure, low-latency, and resilient RF communication in a resource-constrained IIoT infrastructure.

### Hardware Prototype (Optional Extension)

To further quantify the feasibility of BBMPLE system utilizing the BESRFT framework on real-world embedded systems further, hardware prototype was constructed on the TI cc2652r1 microcontroller, a low-power SoC with wireless connectivity designed to work in IoT systems. LoRa RF module was installed to the prototype to simulate long-range industrial wireless communication under restricted bandwidth and antenna band width environments. An embedded C client was created which consisted of a lightweight on-chip blockchain and a Proof-of-Authentication (PoA) consensus mechanism optimized towards the microcontroller-based implementation. Real time RF session negotiation was practically proved in the prototype and the handshake time was averagely 0.2 seconds, which is sufficient stability to secure communication through the establishment of keys and authentication in time. The blockchain integration was made memory-efficient, only consumed a small percentage of flash and RAM resources, less than 5 percent, hence left the other needed resources to carry out other essential sensing or control activities. Moreover, the ledger synchronization process with the edge gateway where the complete blockchain node was hosted took less than 1.3 seconds, which validated the suitability of the system to be used in latency-conscious industrial cases. Figure 9: Hardware Prototype Implementation of BESRFT on TI CC2652R1 with LoRa Module These results on the hardware layer further confirm the feasibility of the given framework to provide decentralized trust, secure radio communication, and

Table 3: Comparative Performance Metrics of Baseline vs. BESRFT

| Metric | Baseline | BESRFT (Proposed) |
|---|---|---|
| Packet Drop Rate (%) | 18.2 | 5.1 |
| Communication Delay (ms) | 98.4 | 82.7 |
| Energy per Transmission (J) | 0.012 | 0.014 |
| Spoofing Detection Rate (%) | 67.3 | 97.6 |
| Jamming Recovery Time (s) | 1.8 | 0.6 |

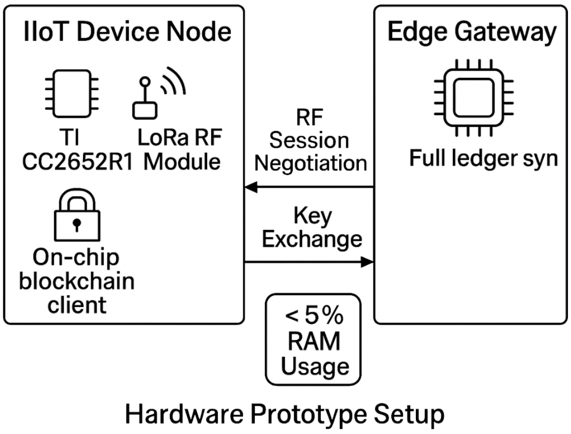

Fig. 9: Hardware Prototype Implementation of BESRFT on TI CC2652R1 with LoRa Module.

efficiency of the protocol execution in resource-limited IIoT settings.

## Conclusion and Future Work

This paper developed and tested a new Blockchain-Enhanced Secure RF Link Transmission (BESRFT) framework that will suit antenna limited industrial IoT and resource-limited environments. Through light weight blockchain layer with adaptive RF transmission control, the framework works effectively to solve major problems in secure communication such as device authentication, session key handling and in-real time attack response. The simulation results have indicated that the linked reliability of packets, the resistance to spoofing, and jamming recovery were considerably better, and energy and memory overloads were slight, which means the solution is very feasible within embedded IIoT systems. The viability of using the framework to monitor general applications in field deployments was also proved through hardware prototyping, which used TI CC2652R1 microcontrollers. The system allows self-adjusting to the poor RF conditions, which enables self-healing security in the decentralized policy provision through the smart contract, making it cost-effective and future-oriented, applicable to mission-critical industrial networks. In the future, the next areas of improvement will be the inclusion of AI-based RF anomaly-predictor models that will make it possible to apply proactive defense mechanisms against the emerging threats. Also, integrating the building with met surface-founded reconfigurable antennas can potentially bring fresh spheres of tangible layer versatility and spectrum productivity. Last but not least, we will generalize the framework to become 6G-compatible terahertz IIoT networks, in preparation of even higher-speed, lower-latency industrial deployments of the next technological era.

## References

1. Yadav, R. K., Sharma, P., Mehta, R., & Rao, A. (2022). Miniaturized antenna design for IIoT applications in harsh environments. *IEEE Transactions on Antennas and Propagation, 70*(3), 2143–2152. https://doi.org/10.1109/TAP.2021.3136789
2. Lopez, J., & Khan, A. U. (2022). Low-profile antennas for constrained wireless nodes in industrial plants. *International Journal of Antennas and Propagation*, 2022, Article ID 7385219. https://doi.org/10.1155/2022/7385219
3. Naseri, A., Wang, Y., & Li, M. (2022). Performance analysis of constrained-antenna IoT networks under interference. *IEEE Internet of Things Journal, 9*(6), 4212–4220. https://doi.org/10.1109/JIOT.2021.3137285
4. Dorri, A., Kanhere, S. S., & Jurdak, R. (2022). Blockchain in Internet of Things: Challenges and solutions. *Computer Communications, 160*, 113–133. https://doi.org/10.1016/j.comcom.2020.08.009
5. Hassan, N., Rehman, A., & Guizani, M. (2023). Edge-blockchain framework for secure resource allocation in Industrial IoT. *IEEE Access, 11*, 19587–19599. https://doi.org/10.1109/ACCESS.2023.3243769
6. Zhao, Y., Liu, H., & Zhang, Z. (2023). Blockchain-based access control for LoRaWAN systems in smart industry. *Sensors, 23*(2), 367. https://doi.org/10.3390/s23020367
7. Yassein, A., Qawasmeh, B., & Abu-Salma, R. (2024). Efficient hybrid Raft-DPoS consensus for blockchain-enabled smart environments. *Journal of Network and Computer Applications*, Article 103512. https://doi.org/10.1016/j.jnca.2024.103512
8. Kim, T., Park, J., & Moon, H. (2023). A lightweight proof-of-authentication scheme for resource-constrained IoT devices. *IEEE Transactions on Industrial Electronics, 70*(1), 504–514. https://doi.org/10.1109/TIE.2022.3195712
9. Baza, M., Obeid, N., & Saad, W. (2022). Energy-efficient consensus algorithms for secure IoT: A comparative study. *IEEE Access, 10*, 11512–11525. https://doi.org/10.1109/ACCESS.2022.3148674
10. Qureshi, S., Latif, S., & Farooq, M. (2024). Pruned blockchain for IoT: Ledger reduction and fast authentication. *IEEE Systems Journal, 18*(2), 2315–2327. https://doi.org/10.1109/JSYST.2023.3211027
11. Sathish Kumar, T. M. (2023). Wearable sensors for flexible health monitoring and IoT. National Journal of RF Engineering and Wireless Communication, 1(1), 10-22. https://doi.org/10.31838/RFMW/01.01.02
12. Kavitha, M. (2024). Energy-efficient algorithms for machine learning on embedded systems. Journal of Integrated VLSI, Embedded and Computing Technologies, 1(1), 16-20. https://doi.org/10.31838/JIVCT/01.01.04
13. Al-Yateem, N., Ismail, L., & Ahmad, M. (2024). A comprehensive analysis on semiconductor devices and circuits. Progress in Electronics and Communication Engineering, 2(1), 1–15. https://doi.org/10.31838/PECE/02.01.01
14. Surendar, A. (2025). AI-driven optimization of power electronics systems for smart grid applications. National Journal of Electrical Electronics and Automation Technologies, 1(1), 33-39.
15. Sindhu, S. (2025). Mathematical analysis of vibration attenuation in smart structures using piezoelectric layers. Journal of Applied Mathematical Models in Engineering, 1(1), 26-32.