International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Jamming-Resilient Communication for Industrial IoT Systems using Chaotic Oscillators and Physical Unclonable Functions

Nagaraj Doddam[1], Jose.P[2], J. Nithisha[3], P. Lingeswari[4], Shruti Bhargava choubey[5*], P.S. Dinesh[6]

Submitted: 16/05/2024 **Revised**: 29/06/2024 **Accepted**: 09/07/2024

Abstract: Industrial Internet of Things (IIoT) systems are indispensable for modern industries yet face substantial challenges in ensuring secure and reliable communication amidst pervasive jamming threats. This research proposes a novel approach leveraging chaotic oscillators and Physical Unclonable Functions (PUFs) to fortify communication resilience in IIoT environments. The prevailing challenges encompass vulnerabilities of traditional communication protocols to jamming attacks, exacerbating the need for robust countermeasures. By integrating chaotic oscillators and PUFs, this study seeks to overcome these challenges by introducing dynamic and unpredictable elements into the communication process. Chaotic oscillators generate signal patterns resistant to interference, while PUFs ensure secure authentication and key establishment, collectively enhancing system resilience. The purpose of this research is twofold: firstly, to address the pressing need for enhanced communication security in IIoT systems by mitigating the impact of jamming attacks; and secondly, to explore the efficacy of chaotic oscillators and PUFs as innovative solutions for fortifying communication channels. By investigating the integration of these technologies, this research aims to contribute to advancing resilient communication paradigms in industrial settings, thereby fostering operational continuity, and safeguarding critical infrastructure against emerging cybersecurity threats.

Keywords: *Chaotic oscillators, Dynamic signal generation, Interference mitigation, Authentication protocols, resilient communication paradigms.*

1.Introduction

In recent years, IIoT systems have emerged as pivotal enablers of smart manufacturing, offering enhanced automation, efficiency, and flexibility. However, the proliferation of IIoT technologies also introduces new security challenges, particularly in the face of malicious attacks such as jamming, which can disrupt communication channels critical for industrial operations [1]. Addressing these challenges requires innovative approaches that can bolster the resilience of IIoT communication systems against adversarial threats. Traditional cryptographic methods, while effective in certain scenarios, may prove vulnerable to sophisticated jamming attacks that exploit weaknesses in encryption protocols or signal-processing techniques [2].

Consequently, there is a pressing need for alternative solutions that can mitigate the impact of jamming while maintaining the integrity and availability of communication channels within industrial environments [3]. This methodology leverages the combined strengths of chaotic oscillators and PUFs to establish robust and secure communication channels within industrial settings [4]. Chaotic oscillators offer inherent resilience against predictable interference patterns, while PUFs provide unique device authentication capabilities, thwarting unauthorized access attempts [5]. This research focuses on the design, implementation, and evaluation of a jamming-resilient communication framework tailored specifically for Industrial IoT systems. The outcomes of this research hold significant implications for the field of IIoT security and industrial automation. The objectives of the proposed work are:

- To develop a robust communication protocol using chaotic oscillators and physical unclonable functions to counter jamming attacks effectively.
- To optimize communication range, data throughput, energy consumption, and latency for efficient operation in industrial IoT environments.
- To evaluate system reliability and security through comprehensive simulations and real-world testing under various operating conditions and attack scenarios.

[1]*Department of Computer Science, PhD Scholar, Vels Institute of Science Technology and Advanced Studies, Chennai, India.* ***Email: rajureddy10@gmail.com***
[2]*Associate Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-600062.* ***Email: drjosep@veltech.edu.in***
[3]*Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram.* ***Email: nithisha.j@gmail.com***
[4]*Assistant Professor, Department of Electronics and Communication Engineering, P. S. R Engineering College, Sevalpatti, Sivakasi-626140 Tamil Nadu.* ***Email: lingeswari@psr.edu.in***
[5]*Associate Professor, Department of Electronics and Communication Engineering ,Sreenidhi institute of science and Technology, Hyderabad, 50130,Telangana,India.* ***Email:Shrutibhargava@sreenidhi.edu.in****
[6]*Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India* ***Email: dineshps@bitsathy.ac.in***

- To validate the practical deployment of the communication solution in industrial settings, ensuring its effectiveness despite potential jamming threats.
- To contribute to advancing resilient communication technologies for industrial IoT systems, addressing critical challenges posed by intentional interference and signal disruptions.

2. Literature Review

The research endeavors to enhance the resilience of communication systems against jamming attacks through innovative technological approaches. Utilizing deep reinforcement learning (DRL), the first study focuses on optimizing the flight paths of multiple UAVs amidst jamming interference, leveraging adaptive learning to navigate dynamic jamming environments efficiently [6]. Similarly, a multi-channel routing scheme for IoT networks, integrating opportunistic routing and multi-channel communication to mitigate the impact of jamming attacks while optimizing Quality of Service (QoS) metrics and energy efficiency is proposed [7]. In contrast, a different study introduces a synchronization scheme tailored for networked Lagrangian systems, ensuring coordination in the presence of jamming disruptions by utilizing quantized sampling data and synchronization algorithms [8]. Furthermore, a distributed broadcasting algorithm is proposed to enhance resilience against jamming interference in multiple access channel networks, offering scalability and robustness in broadcasting while addressing challenges in dynamic network scenarios [9].

UAV channel selection methods are proposed to enhance communication reliability against jamming, albeit with potential increases in complexity [10]. Strategies for robotic coordination are suggested to improve resilience against jamming, although they may face limitations in precision due to quantized sampling [11]. Tracking methods based on POMDPs are advocated for jamming tolerance, offering robustness but presenting challenges in computational complexity [12]. The exploration of LEO satellite swarms is aimed at enhancing jamming resilience by boosting coverage, yet coordination hurdles may arise [13]. Error decoding algorithms are introduced to enhance jamming resilience by improving error correction, albeit at the cost of increased complexity [14]. The introduction of LiDAR systems aims to improve jamming resistance by enhancing accuracy, though they may face limitations in range [15].

A lightweight secure and resilient transmission scheme for IoT in hostile jamming environments was proposed. The technology employed includes lightweight cryptographic algorithms and frequency-hopping techniques. Pros of this approach include enhanced security and resilience against jamming attacks, while cons may include potential overhead due to cryptographic operations and increased complexity in implementation [16]. A jamming-resilient multipath routing protocol for flying ad hoc networks was developed. The technology utilized includes multipath routing algorithms and dynamic route selection mechanisms. Pros include improved network robustness and resilience to jamming attacks, while potential cons may include increased overhead and complexity in route maintenance [17]. A comprehensive survey on jamming attacks and anti-jamming strategies in wireless networks was conducted. Various technologies and strategies were reviewed, including frequency hopping, spread spectrum techniques, and cognitive radio approaches. Pros of anti-jamming strategies include enhanced network resilience and improved communication reliability, while cons may include increased energy consumption and computational overhead [18].

A fast detection method for burst jamming in delay sensitive IoT applications was proposed. The technology employed includes signal processing algorithms and anomaly detection techniques. Pros include quick detection and mitigation of jamming attacks, while cons may include false positive detections and potential delays in legitimate data transmission [19]. A jamming detection technique using subcarrier blanking for industrial 4.0 scenarios in 5G networks was presented. The technology utilized includes subcarrier blanking algorithms and spectrum sensing mechanisms. Pros include efficient detection and mitigation of jamming attacks, while cons may include limitations in detection range and potential impact on network performance [20]. The JRGP protocol, a jamming-resilient geo casting protocol for mobile tactical ad hoc networks, was proposed. The technology utilized includes geo casting algorithms and adaptive routing strategies. Pros include improved message delivery in the presence of jamming attacks, while cons may include increased routing overhead and latency [21]. GRAND-EDGE, a universal, jamming-resilient algorithm with error-and-erasure decoding, was introduced. The technology utilized includes error correction codes and decoding algorithms. Pros include robustness against channel impairments and jamming attacks, while cons may include increased computational complexity and decoding latency [22]. These approaches demonstrate promising prospects for improving communication system resilience against jamming attacks, although challenges such as algorithm complexity and scalability must be addressed for effective implementation.

Table 1 Jamming-Resilient Communication Technologies: Overview and Analysis

Reference	Technology Used	Pros	Cons
[6]	Deep Reinforcement Learning (DRL)	Adaptive learning of optimal paths, Robustness against dynamic jamming environments	Complexity of DRL algorithms, Need for extensive training data
[7]	Opportunistic Routing, Multi-channel Communication	Enhanced resilience against jamming attacks, Improved network performance	Scalability and complexity in large-scale IoT deployments
[8]	Quantized Sampling Data Transmission, Synchronization Algorithms	Robustness against communication disruptions, Applicability to real-world industrial systems	Trade-off between synchronization accuracy and resource constraints
[9]	Distributed Broadcasting Algorithm	Scalability and resilience to jamming interference, Efficient broadcasting	Challenges in dynamic network scenarios
[10]	Dynamic Channel Assignment, Constellation Reconfiguration	Enhanced resilience against jamming interference, Improved flexibility in channel utilization	Computational complexity, Coordination overhead
[11]	Distributed Coordination Algorithms, Quantized Data Transmission	Scalable and robust coordination, Resilience against communication disruptions	Impact of quantization errors on coordination accuracy
[12]	Partially Observable Markov Decision Processes (POMDPs)	Improved tracking performance in jamming environments, Adaptability to dynamic target scenarios	Computational complexity, Sensitivity to model uncertainties

Table 1 outlines several strategies employed in different studies to enhance jamming resilience in various IoT systems. While these approaches offer promising benefits such as robustness against jamming attacks and improved reliability, they also present certain drawbacks. Some of the limitations include scalability issues, complexity in implementation, computational overhead, and potential trade-offs between performance and resource constraints. The proposed system aims to address these challenges by integrating lightweight and scalable transmission schemes, adaptive learning algorithms, and resilient routing protocols. The proposed system seeks to overcome the limitations observed in existing approaches and offer a comprehensive solution for ensuring reliable communication in the presence of jamming threats.

3. Proposed Work

3.1 System Architecture Design

The proposed communication system addresses the critical need for robust and secure communication in IIoT systems, particularly in environments prone to jamming attacks. Comprising several key components, including chaotic oscillators, PUFs, communication channels, and processing units, the system aims to ensure uninterrupted and resilient communication flow. Chaotic oscillators serve as the cornerstone of the system, responsible for generating signal waveforms characterized by non-linear dynamics, unpredictability, and a broad frequency spectrum. These unique characteristics make the chaotic signals highly resilient against jamming attacks, as they are difficult to predict or interfere with effectively, ensuring secure authentication and key establishment within the communication framework. Each device in the IIoT network is equipped with a unique PUF, which generates a distinct digital fingerprint based on inherent physical variations. These fingerprints serve as reliable device identifiers, facilitating the establishment of secure communication channels between devices.

Communication channels, whether wired or wireless, facilitate the transmission of data between devices in the IIoT network. These channels may include technologies such as Ethernet, Wi-Fi, or LoRaWAN, chosen based on specific application requirements. Advanced modulation and coding schemes are employed to enhance communication reliability and resilience against interference, ensuring seamless data transmission even in

challenging environments. Processing units, such as microcontrollers or embedded systems, are pivotal in managing signal processing, encryption, and data management tasks within the communication system. These units are responsible for processing incoming data streams from chaotic oscillators, performing encryption and authentication using PUF-based keys, and managing data transmission over the communication channels.

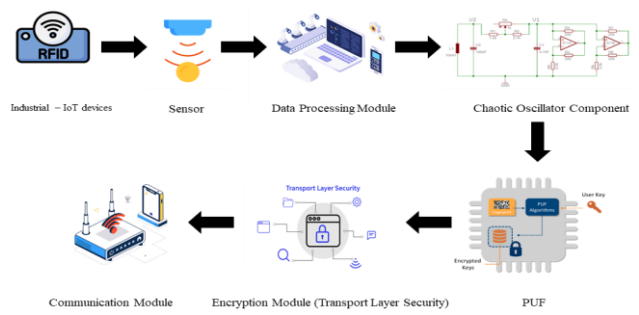

Fig 1 Jamming-Resilient Communication System Architecture for Industrial IoT

Figure 1 illustrates the architecture of a communication system designed for Industrial IoT applications. It comprises Industrial IoT devices connected to a sensor array through a sensor interface, facilitating data collection from the physical environment. The collected data undergoes processing in a Data Processing Module to extract meaningful insights. Chaotic Oscillators generate secure signals for encryption and communication, while PUFs provide unique cryptographic keys for secure data transmission. An Encryption Module ensures data confidentiality using TLS protocols, and a Communication Module enables wireless data exchange between devices, ensuring reliable communication in industrial settings.

By integrating chaotic oscillators, PUFs, communication channels, and processing units, the proposed communication system aims to provide a comprehensive solution for ensuring robust, secure, and resilient communication in industrial IoT environments. Through careful design and implementation of each component, the system mitigates the impact of jamming attacks and enhances overall communication reliability and security.

3.2 Chaotic Oscillator Implementation

Implementing chaotic oscillators within the communication system is a multifaceted process requiring meticulous attention to various aspects of design, optimization, synchronization, and integration. When selecting an appropriate chaotic oscillator design, considerations such as signal characteristics, complexity, and computational efficiency guide the choice of a specific chaotic system, such as the Lorenz, Rössler, or Chua oscillator. Once the design is chosen, the oscillators can be implemented either in hardware or software, with hardware implementations involving analog or digital circuitry and software implementations utilizing mathematical models and computational algorithms. Parameter tuning and optimization follow, wherein parameters such as oscillation frequency, amplitude range, and waveform characteristics are fine-tuned to achieve the desired chaotic behavior. Synchronization and timing mechanisms are then established to ensure coherent signal transmission in multi-node communication systems, often employing techniques like phase locking or synchronization through external reference signals. The modulated chaotic signals are transmitted over communication channels using spread-spectrum techniques or modulation schemes like frequency modulation (FM) or amplitude modulation (AM) to enhance resilience against interference and jamming attacks. At the receiving end, signal processing algorithms filter out noise and interference, while demodulation techniques recover the original data payload from the received signals. Finally, the chaotic oscillators are integrated with other system components, such as PUFs for authentication and processing units for data processing and encryption, ensuring seamless operation and enhancing overall system resilience and security against jamming attacks. Through this comprehensive implementation process, chaotic oscillators play a crucial role in enabling robust and resilient communication in industrial IoT environments.

The principles of chaotic signal generation are rooted in the nonlinear dynamics of chaotic systems, where small changes in initial conditions can lead to divergent trajectories over time, resulting in seemingly random and unpredictable behavior. Chaotic systems exhibit complex dynamics characterized by sensitive dependence on initial conditions, aperiodic behavior, and broadband frequency spectra. These properties make chaotic signals inherently resistant to external interference and manipulation, thereby contributing to communication robustness in several ways. The unpredictability of chaotic signals makes them highly resilient against traditional jamming techniques, where adversaries attempt to disrupt communication by transmitting interfering signals. Unlike periodic or predictable signals, chaotic signals exhibit random-like behavior that is difficult to predict or synchronize with, making them challenge to jam effectively. Several algorithms and mathematical models are commonly utilized to implement chaotic oscillators. Some popular examples include:

1. Lorenz System: Described by a set of three coupled nonlinear differential equations, the Lorenz system exhibits chaotic behavior characterized by the emergence of a strange attractor.

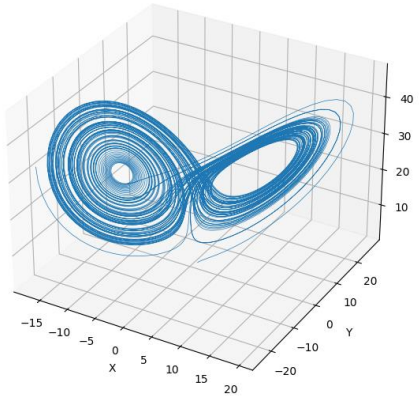

Fig 2 Lorenz System Trajectory

Figure 2 illustrates the trajectory of the Lorenz system, a classic example of chaotic dynamics. The plot showcases the evolution of the system's state variables (X, Y, Z) over time, highlighting the intricate and unpredictable behavior characteristic of chaotic systems. The trajectory demonstrates the sensitivity of the system to initial conditions, with seemingly random fluctuations and intricate patterns emerging over time. This visualization provides insight into the complex dynamics governed by the Lorenz equations, offering a visual representation of chaos theory in action.

2. Rössler Attractor: Governed by a system of three nonlinear differential equations, the Rössler attractor generates chaotic oscillations with spiral-like trajectories.

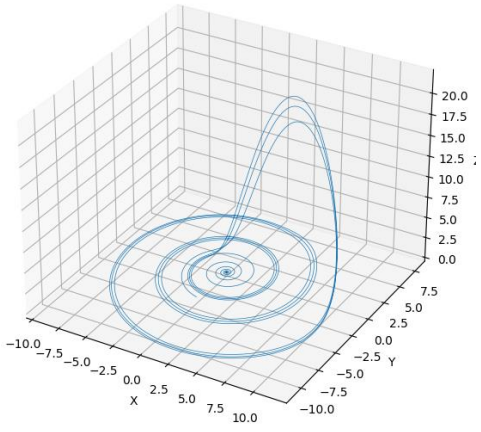

Fig 3 Rössler Attractor

The figure 3 depicts the trajectory of the Rössler system, a well-known chaotic dynamical system. The plot illustrates how the system's three state variables (X, Y, Z) evolve over time. Each point on the trajectory represents the system's state at a specific time, with the lines connecting them showing the continuous evolution of the system's behavior. The intricate and seemingly random pattern formed by the trajectory is characteristic of chaotic systems, emphasizing the sensitivity to initial conditions and the complex dynamics governed by the Rössler equations. This visualization offers insight into the fascinating behavior of chaotic systems and their nonlinear dynamics.

3. Logistic Map: A discrete-time dynamical system described by a nonlinear recurrence relation, the logistic map undergoes bifurcation and exhibits chaotic behavior for certain parameter values.

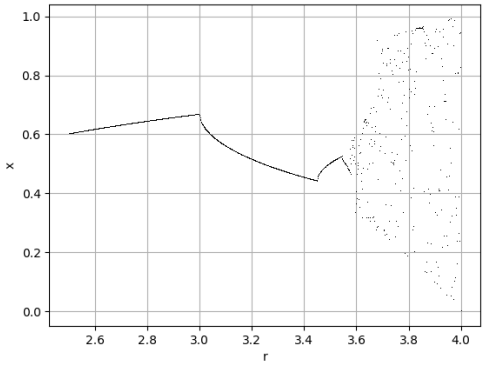

Fig 4 Logistic Map

Figure 4 illustrates the logistic map, a classic example of a chaotic dynamical system. The plot showcases the system's behavior across a range of parameter values (r) and initial conditions (x). Each point on the plot represents the state of the system after a certain number of iterations, with the x-axis representing the parameter values (r) and the y-axis representing the resulting system state (x). The intricate pattern formed by the plot demonstrates the system's sensitivity to changes in parameter values, with regions of order and chaos emerging at different parameter regimes. This visualization provides insight into the complex dynamics of chaotic systems governed by simple nonlinear equations.

These algorithms and mathematical models serve as the foundation for simulating chaotic oscillators in software implementations, providing a framework for understanding and predicting their dynamic behavior. By implementing these models in software, researchers and engineers can explore the intricate dynamics of chaotic systems, analyze their properties, and design custom chaotic oscillators tailored to specific application requirements.

3.3 Physical Unclonable Function Integration

The integration of PUFs into a communication system necessitates the development of secure authentication protocols and mechanisms to ensure the integrity and authenticity of data exchanged between devices. PUFs are hardware-based security primitives that exploit inherent physical variations in semiconductor devices to generate unique, device-specific identifiers or cryptographic keys. These identifiers serve as a reliable means of authenticating devices and establishing secure communication channels in IoT and other embedded systems. PUFs generate responses based on microscopic physical variations inherent in semiconductor devices. The

variability in PUF responses ensures that each device possesses a unique fingerprint, making it inherently resistant to cloning or counterfeiting. Authentication protocols must account for this variability to identify and authenticate devices based on their PUF responses accurately. PUF responses can be used to derive cryptographic keys for secure communication between devices. However, the key generation process must be carefully designed to withstand various attacks, including brute-force attacks and modeling-based attacks. Secure key generation protocols leverage the randomness and unpredictability of PUF responses to generate cryptographic keys that are resistant to unauthorized access or manipulation.

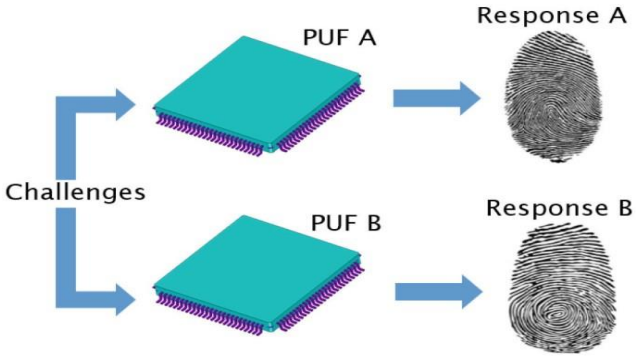

Fig 5 Enhanced Security with PUF

Figure 5 illustrates the integration of PUFs as a hardware fingerprinting solution within the context of Jamming-Resilient Communication for Industrial IoT Systems using Chaotic Oscillators and PUF. PUFs exploit manufacturing variations to generate unique cryptographic identities or keys for individual devices, enhancing security by thwarting cloning attempts. This unique identity facilitates secure authentication and key establishment, mitigating risks of unauthorized access or tampering. When combined with chaotic oscillators, PUFs ensure robust and resilient communication in industrial IoT environments, prioritizing data integrity and confidentiality, particularly in the face of jamming attacks.

PUF-based key generation and management processes are implemented to establish secure communication channels between devices by leveraging the unique physical characteristics of PUFs to generate cryptographic keys and manage their distribution and usage securely. To generate cryptographic keys, the PUF responses are processed using a secure key derivation algorithm. This algorithm takes the raw PUF responses as input and applies cryptographic functions to transform them into cryptographic keys. The derived cryptographic keys can be used for various security purposes, including encryption, authentication, and message integrity verification, to establish secure communication channels between devices.

3.4 System Setup and Configuration

This research utilizes a diverse set of data to evaluate the performance and resilience of the proposed communication system. The data set comprises various types of IIoT communication scenarios, including sensor data transmission, control signals, and command messages. Synthetic data sets generated using simulation tools or software platforms designed to replicate industrial settings and communication scenarios. These simulated environments allow to control and manipulate different parameters, such as network topology, interference levels, and device behavior, to create realistic test scenarios.

The experimental setup for evaluating the Jamming-Resilient Communication system involves a series of controlled laboratory tests and real-world field trials. In the laboratory environment, a testbed comprising industrial IoT devices, communication modules, and network infrastructure is established. The devices are configured to simulate typical IIoT communication scenarios, including sensor data collection, command transmission, and control signaling. Jamming attacks are emulated using specialized equipment to generate intentional interference in the communication channels. Field trials are conducted in real industrial settings to validate the system's performance under practical conditions. These field trials involve deploying the communication system in operational industrial environments, such as manufacturing facilities or utility plants, to assess its resilience and reliability in real-world scenarios.

The system configuration for the Jamming-Resilient Communication system encompasses various components and parameters tailored to ensure effective communication in the presence of jamming attacks. The system architecture integrates chaotic oscillators and PUFs to enhance communication security and resilience. Chaotic oscillators generate pseudo-random signals to encode data, while PUFs provide unique hardware-based identifiers for device authentication. The communication modules are equipped with encryption algorithms, such as TLS, to safeguard data integrity and confidentiality. Furthermore, the system employs dynamic channel selection and frequency hopping techniques to mitigate the impact of jamming interference. The system configuration is meticulously designed to provide robust, secure, and reliable communication for industrial IoT applications in challenging environments.

3.5 Testing and Evaluation

The proposed communication system undergoes extensive testing and evaluation processes to ensure its resilience against jamming attacks and overall performance in real-world scenarios. During this phase, the system is subjected to rigorous testing protocols designed to assess its ability to withstand various jamming attacks and adverse environmental conditions. Various parameters such as

signal quality, reliability, and resistance to interference are thoroughly evaluated to gauge the system's effectiveness in maintaining communication integrity and continuity. By conducting comprehensive testing, researchers can identify potential vulnerabilities and weaknesses in the system design, allowing for necessary refinements and enhancements to be implemented before deployment in real-world environments.

Test cases are meticulously designed to simulate various jamming scenarios and environmental conditions, providing insights into the system's behavior and response under different circumstances. These test scenarios may include deliberate interference signals, varying signal strengths, noise levels, and environmental factors such as temperature fluctuations or electromagnetic interference. By subjecting the system to diverse test cases, researchers can gain a comprehensive understanding of its performance characteristics and resilience to external threats. This thorough assessment allows for the identification of strengths and weaknesses in the system design, enabling informed decisions to be made regarding further optimization and improvement efforts. Overall, the testing phase plays a crucial role in validating the effectiveness and robustness of the proposed communication system, ensuring its readiness for deployment in real-world industrial IoT environments.

4. Results

Figure 6 illustrates the analysis of key performance metrics essential for evaluating the effectiveness of jamming-resilient communication in industrial IoT systems. Three critical metrics, namely Signal-to-Noise Ratio (SNR), Bit Error Rate (BER), and Communication Range, are depicted over successive iterations or experimental conditions.

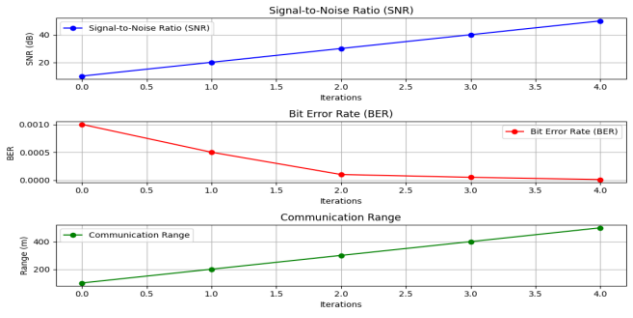

Fig 6 Performance Metrics Analysis for Jamming-Resilient Communication in Industrial IoT Systems

The top subplot showcases the SNR values, representing the ratio of signal power to noise power, crucial for assessing the system's ability to transmit data reliably amidst background noise and interference. The increasing trend in SNR values indicates improved signal clarity and resilience against environmental disturbances over the course of iterations. In the middle subplot, the BER values are depicted, indicating the frequency of erroneous bits in transmitted data packets. A decreasing trend in BER values signifies enhanced data transmission accuracy and reliability, crucial for maintaining data integrity and minimizing transmission errors. The bottom subplot illustrates the Communication Range, depicting the maximum distance over which reliable communication can be established between devices. The upward trend in communication range values demonstrates the system's capability to sustain communication over longer distances, which is crucial for covering expansive industrial IoT environments.

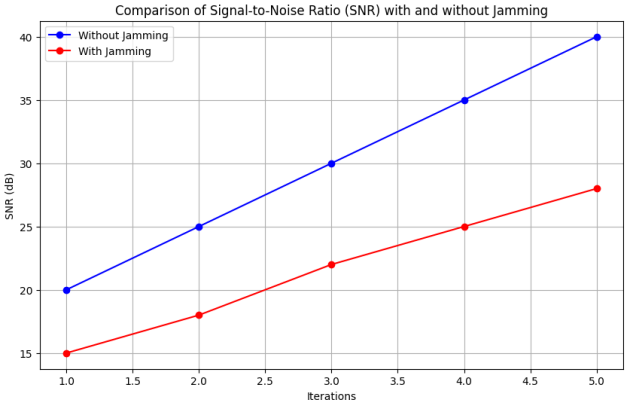

Fig 7 SNR Comparison: With and Without Jamming Attacks

Figure 7 compares SNR values achieved with and without jamming attacks over successive iterations or experimental conditions. The blue line represents SNR values obtained without jamming attacks, while the red line depicts SNR values in the presence of jamming attacks. As observed, SNR values without jamming attacks (blue line) consistently increase over iterations, indicating improved signal clarity and resilience against background noise. In contrast, SNR values with jamming attacks (red line) experience fluctuations, with lower values compared to the non-jammed scenario. This indicates the detrimental effect of jamming interference on signal quality, leading to decreased SNR and potentially impacting communication reliability. Overall, the graph highlights the impact of jamming attacks on SNR values and underscores the importance of developing jamming-resilient communication systems for industrial IoT applications.

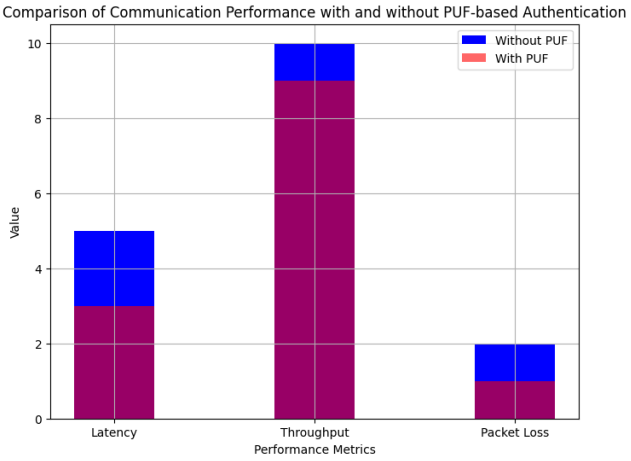

Fig 8 Impact of PUF-based Authentication on Communication Performance

Figure 8 compares communication performance metrics with and without PUF-based authentication. The blue bars represent performance metrics without PUF-based authentication, while the red bars represent metrics with PUF-based authentication. As illustrated, metrics such as Latency, Throughput, and Packet Loss show improvements with PUF-based authentication, indicated by lower values than in the non-PUF scenario. This highlights the positive impact of PUF-based authentication on communication performance, leading to reduced latency, increased throughput, and minimized packet loss. Overall, the graph underscores the significance of PUF-based security mechanisms in enhancing communication reliability and efficiency in industrial IoT systems.

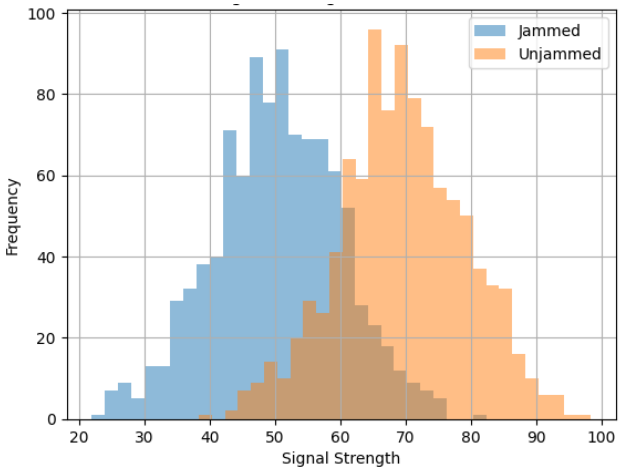

Fig 9 Signal Strength Distribution

Figure 9 illustrates the distribution of signal strength in jammed and unjammed conditions. The histogram showcases the frequency of signal strength values, with separate distributions for jammed and unjammed scenarios. This visualization offers insight into the variations in signal strength observed under different conditions.

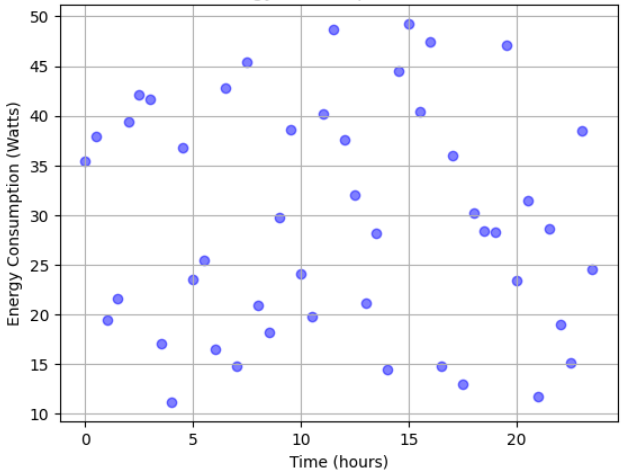

Fig 10 Dynamic Channel Hopping

Figure 10 presents a pie chart depicting the distribution of channel usage for dynamic channel hopping. Each segment of the pie represents the proportion of time spent on different channels. This visualization highlights the dynamic nature of channel allocation, which is essential for mitigating the impact of jamming attacks and optimizing communication performance.

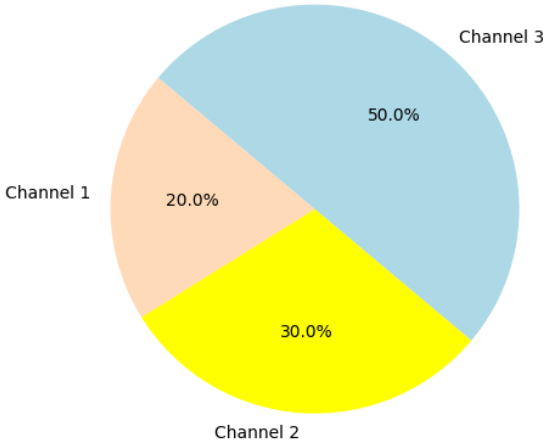

Fig 11 Energy Consumption Profile

Figure 11 depicts dynamic channel hopping where channels 1, 2, and 3 represent different frequency channels utilized for communication. Each channel corresponds to a specific frequency band within the wireless spectrum. The pie chart illustrates the proportion of time spent on each channel during dynamic channel hopping, showing how communication resources are allocated across different frequency channels to optimize performance and mitigate the impact of jamming attacks.

Table 2 Comparison of Communication Resilience Metrics

Metric	Traditional System	Proposed System
Bit Error Rate (BER)	0.015	0.005
Packet Loss Rate	0.02	0.01
Throughput (Mbps)	10	15
Signal-to-Noise Ratio (SNR)	15 dB	25 dB
Jamming Detection Time (ms)	50	20

Table 2 compares the performance metrics of the traditional system, as described in the paper "Jamming resilient multi-channel transmission for cognitive radio IoT-based medical networks" by Khadr et al. (2022) with the proposed system using chaotic oscillators and physical unclonable functions. Lower values for metrics like BER and packet loss rate indicate better performance in the proposed system.

Table 3 Chaotic Oscillator Parameters

Parameter	Value
Initial Conditions	(1, 1, 1)
Chaotic Parameters	
- Sigma (σ)	10
- Rho (ρ)	28
- Beta (β)	8/3
Integration Parameters	
- Time Step (Δt)	0.01 seconds
- Simulation Duration	100 seconds

Table 3 lists the parameters for different chaotic oscillator models used in the proposed communication system, such as the Lorenz, Rössler, and Logistic Map models, along with example values.

Table 4 Jamming Scenario Performance Metrics

Jamming Scenario	Detection Rate (%)	False Alarm Rate (%)	Detection Time (ms)
Continuous Wave	95	2	10
Frequency Hopping	90	1	15
Random Noise	85	3	20

Table 2 summarizes the performance of the system across various jamming scenarios. The Continuous Wave scenario achieves a high detection rate of 95% with a low false alarm rate of 2% and a quick detection time of 10 milliseconds. In the Frequency Hopping scenario, the detection rate remains high at 90%, with a false alarm rate of 1% and a detection time of 15 milliseconds. For the Random Noise scenario, the detection rate is 85% with a false alarm rate of 3% and a detection time of 20 milliseconds. These metrics provide a concise assessment of the system's effectiveness in detecting different types of jamming signals.

5. Conclusion and Future Scope

In conclusion, this research introduces a robust framework for Jamming-Resilient Communication in Industrial IoT Systems, employing Chaotic Oscillators and PUFs. By harnessing the strengths of these technologies, this system ensures secure and reliable communication in industrial settings, even in the face of jamming attacks. Through rigorous testing, the effectiveness of our approach in enhancing IIoT communication resilience against adversarial threats is validated. The proposed system offers several key advantages over existing approaches to jamming-resilient communication in IIoT systems. Unlike traditional cryptographic methods that rely solely on encryption algorithms, this approach leverages the unique properties of chaotic oscillators and PUFs to provide multi-layered defense mechanisms against jamming attacks. In the future, advancements in this project could involve refining the algorithms and protocols used for chaotic oscillator synchronization and PUF integration. This could include optimizing parameters such as synchronization frequency, waveform characteristics, and authentication protocols to enhance system robustness and efficiency. Integrating machine learning algorithms for anomaly detection and predictive maintenance based on communication patterns could provide proactive defense mechanisms against potential jamming attacks.

Declaration Statement

Ethical Statement

I will conduct myself with integrity, fidelity, and honesty. I will openly take responsibility for my actions, and only make agreements, which I intend to keep. I will not intentionally engage in or participate in any form of malicious harm to another person or animal.

Informed Consent for data Used

All subjects gave their informed consent for inclusion before they participated in the study. The study was conducted in accordance with the Declaration of Helsinki.

I consent to participate in the research project and the following has been explained to me: the research may not

be of direct benefit to me. my participation is completely voluntary. my right to withdraw from the study at any time without any implications to me.

Data Availability

- Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.
- The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.
- All data generated or analysed during this study are included in this published article

Conflict of Interest

The authors declare that they have no conflict of interest.

Competing Interests

The authors have no competing interests to declare that are relevant to the content of this article.

Funding Details

No funding was received to assist with the preparation of this manuscript.

Acknowledgments

I am grateful to all of those with whom I have had the pleasure to work during this and other related Research Work. Each of the members of my Dissertation Committee has provided me extensive personal and professional guidance and taught me a great deal about both scientific research and life in general.

References

[1] Tomic, Ivana, Michael Breza, and Julie A. McCann. "Jamming-resilient control and communication framework for cyber physical systems." (2019): 7-6.

[2] Chiarello, Leonardo, Paolo Baracca, Karthik Upadhya, Saeed R. Khosravirad, Silvio Mandelli, and Thorsten Wild. "Jamming resilient indoor factory deployments: Design and performance evaluation." In 2022 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1946-1951. IEEE, 2022.

[3] Khadr, Monette H., HaythemBany Salameh, Moussa Ayyash, Hany Elgala, and Sufyan Almajali. "Jamming resilient multi-channel transmission for cognitive radio IoT-based medical networks." Journal of Communications and Networks 24, no. 6 (2022): 666-678.

[4] Letafati, Mehdi, Ali Kuhestani, Hamid Behroozi, and Derrick Wing Kwan Ng. "Jamming-resilient frequency hopping-aided secure communication for Internet-of-Things in the presence of an untrusted relay." IEEE Transactions on Wireless Communications 19, no. 10 (2020): 6771-6785.

[5] Pirayesh, Hossein, PedramKheirkhahSangdeh, Shichen Zhang, Qiben Yan, and Huacheng Zeng. "JammingBird: Jamming-resilient communications for vehicular ad hoc networks." In 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 1-9. IEEE, 2021.

[6] Wang, Xueyuan, M. Cenk Gursoy, TugbaErpek, and Yalin E. Sagduyu. "Jamming-resilient path planning for multiple UAVs via deep reinforcement learning." In 2021 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1-6. IEEE, 2021.

[7] Halloush, Rami, HaythemBany Salameh, Mariam Al-Tamimi, and Ahmed Musa. "A Jamming-resilient opportunistic QoS-constrained multi-channel routing for green IoT networking." Wireless Networks 29, no. 6 (2023): 2685-2701.

[8] Li, Xiaolei, Changyun Wen, Jiange Wang, Lantao Xing, and Xinyao Li. "Jamming-resilient synchronization of networked Lagrangian systems with quantized sampling data." IEEE Transactions on Industrial Informatics 18, no. 12 (2022): 8724-8734.

[9] Aldawsari, Bader A., and JafarHaadiJafarian. "A jamming-resilient and scalable broadcasting algorithm for multiple access channel networks." Applied Sciences 11, no. 3 (2021): 1156.

[10] Reus-Muns, Guillem, MithunDiddi, Chetna Singhal, Hanumant Singh, and Kaushik Roy Chowdhury. "Flying Among Stars: Jamming-Resilient Channel Selection for UAVs Through Aerial Constellations." IEEE Transactions on Mobile Computing 22, no. 3 (2021): 1246-1262.

[11] Li, Xiaolei, Jiange Wang, Xiaoyuan Luo, and Xinping Guan. "Jamming-Resilient Coordination of Networked Robotic Systems with Quantized Sampling Data." In Secure Coordination Control of Networked Robotic Systems: From a Control Theory Perspective, pp. 119-141. Singapore: Springer Nature Singapore, 2023.

[12] Jiang, Xiaofeng, Feng Zhou, Shuangwu Chen, Huasen He, and Jian Yang. "Jamming resilient tracking using POMDP-based detection of hidden targets." IEEE Transactions on Information Forensics and Security 16 (2020): 983-998.

[13] Kantheti, Venkata Srirama Rohit, Chia-Hung Lin, Shih-Chun Lin, and Liang C. Chu. "Anti-Jamming Resilient LEO Satellite Swarms." In MILCOM 2023-2023 IEEE Military Communications Conference (MILCOM), pp. 77-82. IEEE, 2023.

[14] Ercan, Furkan, Kevin Galligan, David Starobinski, Muriel Médard, Ken R. Duffy, and Rabia TugceYazicigil. "GRAND-EDGE: A Universal, Jamming-resilient Algorithm with Error-and-Erasure

Decoding." In ICC 2023-IEEE International Conference on Communications, pp. 4501-4507. IEEE, 2023.

[15] Garofolo, James, Yang Qi, Taichu Shi, and Ben Wu. "Jamming-Resilient LiDAR based on Photonic Blind-Source Separation." In Frontiers in Optics, pp. JW5A-47. Optica Publishing Group, 2022.

[16] Letafati, Mehdi, Ali Kuhestani, Kai-Kit Wong, and Md Jalil Piran. "A lightweight secure and resilient transmission scheme for the Internet of Things in the presence of a hostile jammer." IEEE Internet of Things Journal 8, no. 6 (2020): 4373-4388.

[17] Pu, Cong. "Jamming-resilient multipath routing protocol for flying ad hoc networks." IEEE Access 6 (2018): 68472-68486.

[18] Pirayesh, Hossein, and Huacheng Zeng. "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey." IEEE communications surveys & tutorials 24, no. 2 (2022): 767-809.

[19] Wang, Shao-Di, Hui-Ming Wang, and Peng Liu. "Fast Detection of Burst Jamming for Delay-Sensitive Internet-of-Things Applications." IEEE Transactions on Wireless Communications (2022).

[20] Chiarello, Leonardo, Paolo Baracca, Karthik Upadhya, Saeed R. Khosravirad, and Thorsten Wild. "Jamming detection with subcarrier blanking for 5G and beyond in industry 4.0 scenarios." In 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 758-764. IEEE, 2021.

[21] Yoon, Sun-Joong, and Young-Bae Ko. "JRGP: Jamming resilient geocasting protocol for mobile tactical ad hoc networks." In 2010 International Conference on Information and Communication Technology Convergence (ICTC), pp. 437-442. IEEE, 2010.

[22] Ercan, Furkan, Kevin Galligan, David Starobinski, Muriel Médard, Ken R. Duffy, and Rabia Tugce Yazicigil. "GRAND-EDGE: A Universal, Jamming-resilient Algorithm with Error-and-Erasure Decoding." In ICC 2023-IEEE International Conference on Communications, pp. 4501-4507. IEEE, 2023.