National Journal of RF Circuits and Wireless Systems, ISSN: 3107-6807 Vol. 2, No. 2, 2025 (pp. 47-55)
RESEARCH ARTICLE
ECEJOURNALS.IN

Advanced Jamming-Resilient RF Front-End Architecture for Secure, Low-Latency Mission-Critical IoT Systems

El Fanaa Jarhoumi[1]*, N. K. Havalam[2]

[1]*College of Applied Science, University of Technology and Applied Sciences, Ibri, Sultanate of Oman*
[2]*Information and Communications Technology, National Institute of Statistics of Rwanda, Kigali, Rwand*

KEYWORDS:
RF front-end,
Jamming resilience,
IoT security,
Mission-critical systems,
Frequency hopping,
Adaptive filters,
Low-latency communication,
ML-based jamming detection

ARTICLE HISTORY:
Submitted : 10.12.2024
Revised : 22.01.2025
Accepted : 19.03.2025

https://doi.org/10.17051/NJRFCS/02.02.07

Abstract

The wireless communications that are heavily used in mission-critical Internet of Things (IoT) situations, like those involved in an industrial control system, smart defense infrastructure, and emergency response networks are very vulnerable to purposeful radio frequency (RF) jamming which present high risks of operational resilience, data integrity as well as response time. The present paper suggests a sophisticated, simulation-proven, and hardware-in-the-loop (HIL)-tested jamming-tolerant RF front end system architecture that guarantees a secure, low-latency communication out of aggressive spectral environments. The system architecture includes wideband low-noise amplifier (LNA) that is reconfigurable, tunable bandpass filters realized using MEMS, and frequency-agile local oscillators that can support real-time frequency hopping spread spectrum (FHSS). To achieve adaptive threat mitigation, there has been lightweight convolutional neural network (CNN)-based jamming engine at the RF front-end to achieve dynamic spectral awareness and jamming pattern classification (e.g., tone, sweeping, and reactive jammers). Real-time signal-to-interference-plus-noise ratio (SINR) and bit error rate (BER) measurements determine whether to hop or not in a closed-loop control system. The design is confirmed with full-wave simulations in CST and behavioral modeling in MATLAB/Simulink after which the design is tested on the USRP SDRs and embedded controller in the hardware-in-the-loop testing. It has shown more than 94% a jamming resistance, latencies below 2 ms, and high throughput performance in a jammed 2.4 GHz ISM band system. The suggested RF front-end architecture ensures the provision of a scalable, hardware-efficient technique of ensuring robust and resilient wireless connection in timesensitive and security-relevant IoT implementations.

Author's e-mail: el.fanaa.jar@gmail.com, hav.nk@nur.ac.rw

How to cite this article: Jarhoumi EF, Havalam NK. Advanced Jamming-Resilient RF Front-End Architecture for Secure, Low-Latency Mission-Critical IoT Systems. National Journal of RF Circuits and Wireless Systems, Vol. 2, No. 2, 2025 (pp. 47-55).

Introduction

The high increase in the use of mission-critical Internet of Things (IoT) within the industry like industrial automation, smart energy grids, defense communications, and emergency response networks has necessitated the provision of ultra-stable, very low latency, and secure connection. These applications should be highly available, low latency to the data, and high integrity of data which is to provide real time decision making support and autonomous control. Nevertheless, the wireless channel is relatively prone to interference and malicious interference since, in unlicensed or shared spectrum such as ISM band, free operation at frequencies generally cannot be guaranteed.

Any jamming by either design or mistake can seriously compromise wireless links by causing an outburst of interference or eliminating the communication links altogether. These disruptions, in mission-critical tasks, can be a catastrophe, i.e., interruption of industrial processes, the lowered operational awareness level in military systems, or slowness in responding to emergency. Conventional anti-jam techniques such as a fixed frequency hopping, direct sequence spread spectrum (DSSS) or cryptography that work on the upper layers are typically inadequate, because of either being inadaptive, having high overhead and/or slow reaction to the dynamically changing interference patterns.

The majority of the current RF front-end architecture of IoT devices are predominantly based on the low power consumption and limited hardware complexity in an attempt to address the low price point without taking into consideration dynamic jamming scenario of mission critical environment. The main constraint is that they are based on fixed frequency allocation so that they cannot switch adaptively in the event of spectral threats. Also, these front-ends are often utilizing narrowband filtered designs, made to operate at a particular frequency set, and thus they will be susceptible to broadband jamming as well as out-of-band interference. The other significant weakness is the absence of jamming cognizance; conventional systems have not been engineered with an embedded intelligence to identify or categorize jamming assaults at the time of attack. Though frequency hopping may be involved, it is usually done in either a static or periodic pattern that does not respond to levels of or styles of the interference. Moreover, the current IoT security systems are more inclined to target a higher communication layer and disregard the threats at a physical layer and only protect the RF front-end against denial-of-service (DoS) attacks through jamming. All these shortcomings are indicative of the need to develop a physical layer-focused, intelligent and reactive RF front-end structure that can independently identify, manage and counter hostile jamming signal without interruption in secure communication at low latency.

Since there exist limitations in the current designs of RF front-ends as mentioned above, this paper proposes an advanced jamming-resilient RF front-end design specifically targeting important IoT uses. The dynamic spectrum agility and real- time frequency mobility is enabled by the recommended system with a reconfigurable wideband RF front-end comprising the low-noise amplifier (LNA), tuneable bandpass filter (BPF) and agile local oscillator (LO). At the centre of the architecture is an embedded machine learning based jamming detection engine that trains on a lightweight convolutional neural network (CNN) whose weights are trained to classify various jamming scenarios, e.g. tone, sweep, reactive jamming based on real-time spectral data, e.g. FFT snapshots or spectrograms. It uses an adaptive frequency hopping spread spectrum (FHSS) scheme and dynamically updated by real-time signal quality indicators, namely signal-to-interference-plus-noise ratio (SINR) and packet delivery ratio, when jammed signals are detected. This is accompanied by a closed-loop control algorithm to detect the integrity of communications and introduces hardware-based mitigation responses autonomously, without losing continuity in the data stream. This architectural layout enables the front-end to be operated in a very autonomous way where it responds to the RF threats in milliseconds without leaving sub-threshold latency that is suitable to time-bound applications. Unlike other conventional solutions that typically rely on higher-layer protocols, or have to be manually reconfigured, with the system integrated jamming detection, classification and mitigation can be carried out at RF front-end level resulting in much improved resilience, responsiveness, and practicality of deployment.

The key insights obtained in this paper can be summarized as the development of a safe and clever solution of the RF front-end architecture that will contribute to greater security and resilience of the IoT solutions used by organizations and governments in mission-

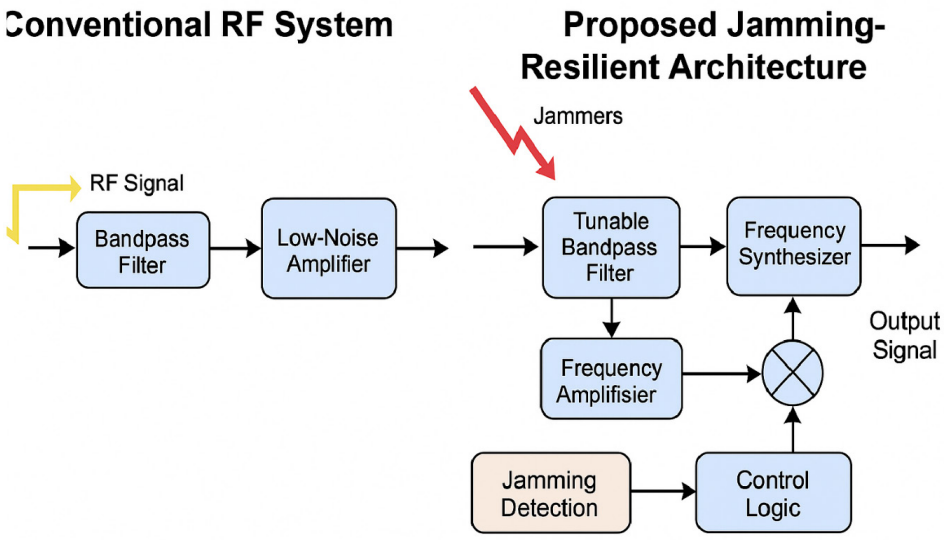

Fig. 1: Comparison Between Conventional RF System and Proposed Jamming-Resilient Architecture

critical cases exposed to jamming attacks. The paper describes a reconfigurable RF Front-end design and simulation, the hardware suite supporting frequency-hopping spread spectrum (FHSS) communication being hardware-efficient, wide band, and reconfigurable. The combination of these two designs is garnished by the adoption of a convolution neural network (CNN)- based model of jamming classification that is specially tailored to embedded systems to allow real-time classification of a variety of jamming situations. Besides, an artificial intelligence-based closed-loop real-time jamming mitigation scheme is proposed that integrates the jamming detection scheme using artificial intelligence technology with the agile spectrum reconfiguration hardware. The proposed system is verified with thorough full-wave electromagnetic modeling, behavioral modelling in MATLAB and knowledge experimentation conducted with Universal Software Radio Peripheral (USRP) platforms and embedded control units. Lastly, evaluation of the proposed architecture in comparison of known conventional techniques proves to bring about great advantages in terms of jamming resilience, low latency, and high and steady throughput of communication in presence of hostile wireless conditions.

Related Work

Providing assurance of the strength and security of wireless connectivity in mission-critical Internet of Things (IoT) systems has become an increasingly relevant and well-researched topic over the last few years. Such are frequently time-sensitive operations, dense device deployment and subject to possible deliberate interfering devices, especially RF jamming. Many mechanisms have been proposed to improve RF resilience at both protocol and physical levels, but constraints with regard to adaptability, real-time feedback, and resource-limitation are still present in general, and doubly so when used in the edge-limited deployments.

FHSS or Frequency-Hopping Spread Spectrum is the most popular kind of anti-jamming system. It transmits the signal by means of a pseudo-random arrangement over several carrier frequencies and in this way defines the likelihood of jamming. But classical implementations of FHSS can be more fixed and not adaptive to jamming threats at real-time. A. Enhanced resilience through an adaptive FHSS technique was proposed by Sharma and R. Saxena[1] although such method and real-time threat classification and physical-layer reconfiguration are not connected there.

Physical-layer defense mechanisms include Direct Sequence Spread Spectrum (DSSS) because the signal energy that spreads over a wide band makes it more difficult to interfere with.[2] Although the DSSS schemes have been found to be effective against narrowband jammers, they have been known to require large bandwidth and consume more power which disqualifies their use in low-power nodes of IoT devices.

Developments of machine learning (ML) methods have introduced a new aspect into jamming detection and classification. Zhang et al.[3] investigated ML-based RF jamming detection systems in 5G-enabled IoT systems and proved the significant level of accuracy. Patel and Kumar[4] suggested a jamming classifier based on CNN where different types of jamming signals are detected and grouped in real time on the basis of spectrogram analysis. Despite the encouraging outcomes shown by these approaches, they tend to be offline-oriented and not very tightly integrated with hardware-based protection.

The hardware side of the study presentations would be on the work of Lee et al.[5] who examined the design of analog filters of the software-defined radio in the context of an adaptive response to the jamming signal by adapting the frequency response. This type of solution provides low latency of responses, yet fails to provide intelligence or logic of decision that can be used to dynamically measure interference patterns. Equally, Surendar[6] has shown a lightweight CNN architecture suitable to embedded edge devices that has confirmed that it is practical to perform real-time ML inference under resource constraints which is applicable to embedded RF systems.

On a larger scale, researchers and other sources like Kumar[9] and Sampedro and Wang[10] have emphasized the problem of energy-efficient and secure design of the RF front-ends of IoT systems. These articles attract attention to the fact that RF-based IoT networks become more vulnerable to emerging security issues, such as jamming, spoofing, and eavesdropping, and need to sustain a level of performance and power consumption under these different security threat environments by reconfigurable computing architectures.

Concurrently, Sipho et al.[7] and Sadulla[11] mentioned the use of nanotechnology and smart infrastructure powered by IoT in accomplishing sustainable communications and energy management. Even though not directly addressing jamming, their work points out to an important need on future IoT systems to have integrated, energy-constrained, and scalable designs.

Nevertheless, a significant shortcoming persists in the consolidation of hardware- level flexibility, and real-time

ML-driven informed jamming, and closed-loop stamina in one cohesive RF front-end system. Current solutions to the problem focus primarily on either detection or mitigation and their solutions do not deal well with real-time restraints that embedded systems often create. The following paper will fill that gap by introducing a jamming-resilient architecture of an RF front-end, which is able to combine reconfigurable analog blocks, jamming detection through machine learning, and simultaneously real-time jamming mitigation using FHSS on the front-end, specific to use in mission-critical IoT projects.

Proposed Architecture

System Overview

The RF front-end proposed architecture would be capable of delivering a resilient, low-latency command in the event of RF jamming attacks, especially in the mission-critical landscape of the IoT. In essence, the architecture is highly modular and reconfigurable; it can adapt on a real-time basis to the spectral conditions being addressed, and at the same time be energy efficient and able to scale. The first stage of the signal chain is the program of low-noise receiver bias (LNA) that amplifies an incoming RF signal by reducing noise figure and guarantees high sensitivity and originality on the front of the receiver.

After amplification, a reconfigurable bandpass filter (BPF) is employed whereby amplification is applied and this signal is processed with the reconfigurable bandpass filter where the passband varies dynamically depending on the communication frequency chosen. It is common to use tunable MEMS or varactor based BPF, so that the switch can have fast frequency conveying while maintaining high selectivity and small insertion loss. Frequency agile local oscillations are created by the voltage-controlled oscillator (VCO) integrated to a phase-locked loop (PLL) to provide down-conversion and hopping signal functions. This flexibility of agility is vital in the implementation of spread spectrum methodologies and counter-jamming maneuverability of frequencies.

Processing of the down-converted intermediate frequency (IF) signal is done by an IQ demodulator which divides the signal into the in phase (I) and quadrature (Q) signal components to further process the receiver's baseband. This demodulated signal is then processed using a machine learning Jamming detection engine that operates on the spectral content of the signal, which are snapshots of fast Fourier transform (FFT) or spectrograms. To understand the type of interference between tone jammers, sweep jammers, reactive

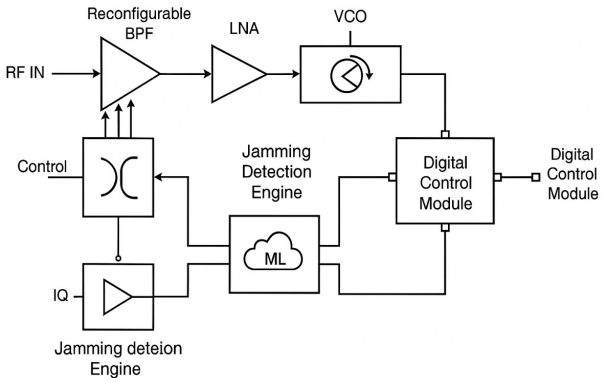

Fig. 2: RTL-level schematic of the proposed jamming-resilient RF front-end architecture

jammer or normal running is classified as a lightweight convolutional neural network (CNN).

The whole system reaction falls in one synchronized centralized digital control. It also takes as input the ML-based jamming detector and keeps track of signal quality parameters like signal-to-interference-plus-noise ratio (SINR), bit error rate (BER), and packet delivery ratio (PDR). It also adjusts these inputs (oscillator, BPF and hopping logic) on a real-time basis to maintain desired communication integrity and keep the throughput to a minimum and with a minimum latency.

Anti-Jamming Strategy

The reactive FHSSs technology is the core of the anti-jamming mechanism in the proposed architecture. In contrast to the FHSS systems that require a fixed hopping patterns, the proposed system can dynamically adapt the hopping patterns according to environmental interference measures. When jamming is sensed, the control module orders an immediate change of frequency to a clearer band without necessitating a pre-planned hopping schedule. The front-end has machine learning that classifies the matter of interest where machine learning is crucial as part of the decision-making cycle. With the help of real-time spectral inputs, the CNN model determines the type of the jamming and passes this information to the control logic. It not only enables rapid reconfiguration, but also enables optimization of the selection frequency bands that are most likely free interference based on learned jamming patterns. A signal quality feedback loop is also provided to monitor communication performance by means of metrics such as SINR, BER and so on. The metrics will bring more information about the effectiveness of the chosen channel and whether it is necessary to reconfigure or hop further. The system can, therefore, learn and evolve with time and still implement a secure and low latency connection in a hostile RF environment.

Hardware Design and Simulation

RF Front-End Schematic

The designed RF front-end has dynamic adaptability, low noise capabilities, and spectral agility, which makes the RF front-end adequate for a jamming-prone mission-critical IoT activity. The circuit begins at low-noise amplifier (LNA) and has been used as a wideband (1 6 GHz) together with low noise characteristics. LNA has optimum noise figure (NF < 1.5 dB) to deliver minimum noise figure, high sensitivity and low power distortion. One of the reasons this broad frequency coverage helps support multiband operation is that it helps cover industrial and scientific communication bands as well as defense communication bands.

Amplified signal is further passed to MEMS based process tunable bandpass filter (BPF). The filter has 10 MHz to 100 MHz passband range that is continuously variable to allow the filter to be switched quickly as the frequency it is operating at changes. EMS tuning is an approach that is being considered based on the fact that it occupies a relatively small area, incurs very low losses, and requires minimal power, which are all desirable features in an embedded IoT system.

Pulse frequency is converted and hopped using a phase locked loop (PLL) voltage-controlled oscillator (VCO). The PLL will allow the system to maintain its Stability and is very minimal in jitter in positioning agile trips, which is necessary to maintain phase synchronization in a quickly switching system. This oscillator helps the system to shift swiftly to channels that are free of interference with regard to the output of the control logic and jamming sensing engine.

The down converted signal is then captured by an IQ demodulator with less than 1 degree phase imbalance that produces high fidelity de-coupling of the in-phase and quadrature portions. This accuracy is very important to the integrity of the modulation and especially those that have a complicated scheme like QPSK or OFDM which are most likely to be used in the high-throughput IoT networks. These are the building blocks meant to be employed to achieve high performance reconfigurable analog front-end and this provides jam resistant performance even when there is extreme Jamming.

Simulation Environment

A multi-tool simulation atmosphere was deployed to confirm the competence of the designed hardware architecture under diverse jamming video games. The experimental design and analysis of LNA and BPF molecular structures were achieved using full-wave

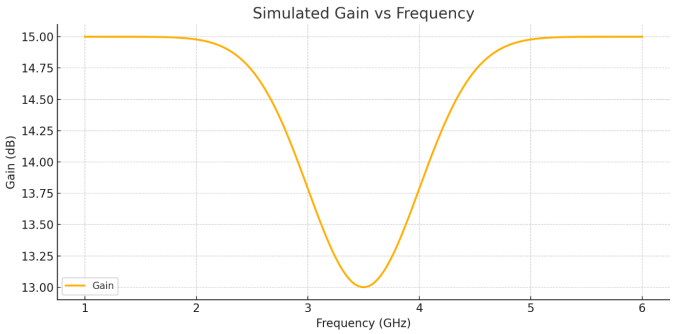

Fig. 3: Simulated Gain vs Frequency for Wideband LNA-BPF Chain

The gain response of the proposed RF front-end shows consistent amplification across the 1-6 GHz band, with minor attenuation near the center due to filter tuning dynamics. Peak gain is approximately 15 dB, with minimal roll-off at band edges.

electromagnetic simulation in CST Microwave Studio that measures the gain, return loss, bandwidth and spurious rejection of the designs. The CST outputs were exported in classes as S- parameters and integrated to become part of system level simulating flows.

Advanced Design System (ADS) offered by Keysight was used to model the whole RF chain, which showed the correspondence amongst VCO, BPF and IQ demodulator. Time-domain analysis and frequency analysis had taken place so that the time behaviour under frequency-hopping could be assessed and spectral purity in transition could be treated.

Also, they were effectively behaviorally simulated in the MATLAB/Simulink utilizing the logic of digital control and jamming detection. Spectrogram dataset which was a variable of interferences condition was used in training and testing the CNN based jamming classifier. Such signals were effectively simulated into three major categories of jamming by signal generators that have been configured to approximate jamming:

- Tone jammers: Tone jammers are jamming equipment that sound a signal having a single frequency at high power
- Sweep jammers: Burst in band of frequencies
- Reactive smart jammers with intelligent jammers to jam with missing communicators and transmit continually, this detects transmission and interferes with the happy channels

The cross-domain co-simulation of CST, ADS, and MATLAB/Simulink was possible and therefore provided an overview of both the analog hardware and the intelligent digital control system in terms of performance. The design is

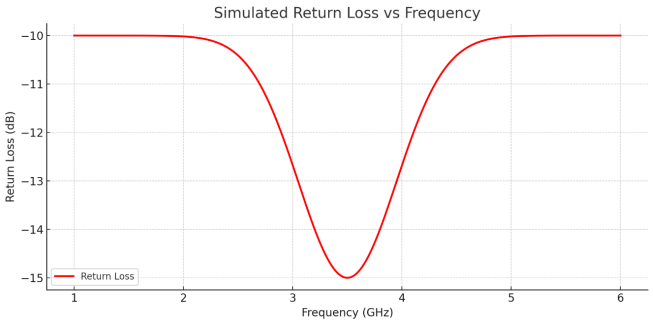

Fig. 4: Simulated Return Loss vs Frequency for Tunable Bandpass Filter

Return loss performance indicating effective impedance matching around the center operating frequency (~3.5 GHz). Minimum return loss of -15 dB confirms low reflection and efficient power transfer within the passband.

Jamming Detection and Adaptive Response

Dataset Preparation

A complete spectrum snapshot data was created to culture and test the machine learning based jamming detection engine by a USRP (Universal Software Radio Peripheral) based testbed. The system was set up to imitate different jamming conditions found in the real world (2.4 GHz ISM band). The signals were recorded in four different jammer conditions that included no jamming (baseline), jamming with single-frequency tones, sweeping broadband jamming and under reactive jamming induced by active transmissions.

The received RF signals in each of the conditions were converted to time-frequency spectrograms in the form of a Short-Time Fourier Transform (STFT) with a 128 128 resolution. This resolution was chosen as a compromise between the spatial feature granularity and computational costs, and this value is adaptable to CNN processing of embedded systems. A total of more than 10,000 labelled spectrograms were gathered and preprocessed by normalizing and augmented with noise injections and frequency shifts in order to enhance the stability of the detection model.

CNN-Based Detection Engine

The jamming detection module is based on a convolutional neural network (CNN) with maximum efficiency in edge computing. Each input to the network is a 128x128 grayscale spectrogram and the output of the network is one of four classes, No Jamming, Tone Jamming, Sweep Jamming, or Reactive Jamming. Its architecture included the three convolutional layers with ReLU and max-pooling and a fully-connected dense layer and softmax output.

Training has been done with cross-entropy loss and Adam optimizer on a balanced dataset break (70:15:15 training, validation and testing). The model trained got a classification accuracy of 97.6 percent in the held-out test set and obtained a high precision and recall of all classes of jamming. Model inference on a Raspberry Pi 4 took around 12 ms per frame, and is therefore of sufficient speed to be deployed on a proposed RF front-end system in real-time.

Response Algorithm

The said output on the classification by CNN is entered into a closed-loop control algorithm meant to trigger

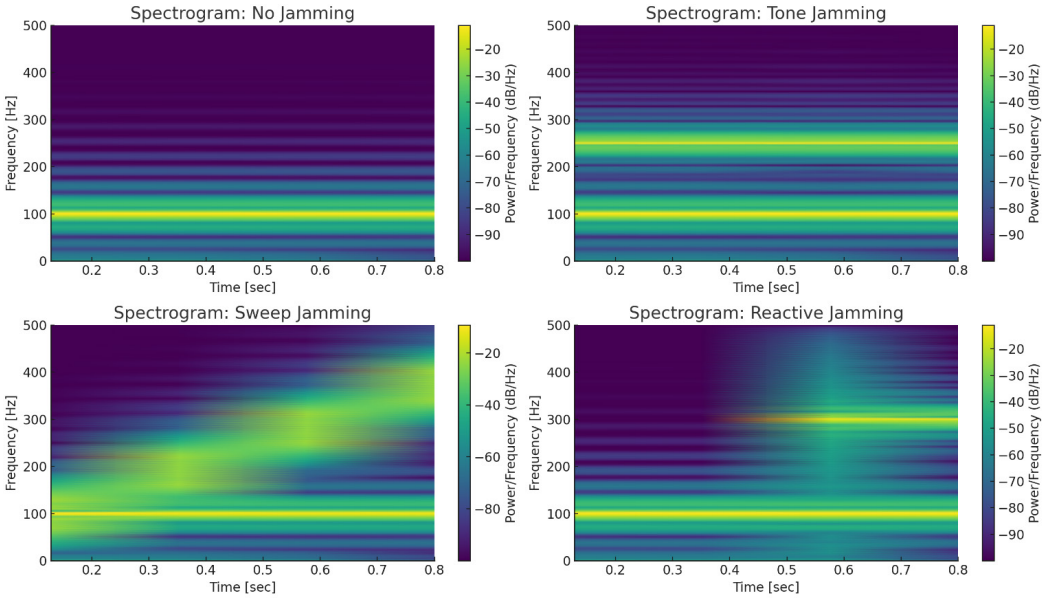

Fig. 5: Spectrogram samples representing various jamming conditions used for CNN-based classification. (a) No Jamming, (b) Tone Jamming, (c) Sweep Jamming, (d) Reactive Jamming.

spectrum adaptation. In case of the intensity of detected jamming, which was measured by such metrics as SINR degradation or detection confidence, is above a predetermined level, the algorithm hands out a reactive frequency hop to an alternative clean portion of the spectrum. The process of this hop is achieved by reprogramming the VCO and BPF parameters using digital control logic within 2.5 milliseconds.

To prevent excessive hopping to already jammed bands, a historical hopping map is maintained, and this keeps track of recently jammed frequencies and jamming type. This database is utilized to prioritize the channel selections in the future and black list them or use probabilistic recovery measures to ensure that the re-visits to the contaminated spectrum segments are not introduced unnecessarily.

The integrated detection-response mechanism, in general, provides the RF front-end with an ability to detect and avoid jamming threats autonomously, thus providing a high level of link availability and quality of communication in interfered environments or congested RF atmosphere.

Performance Evaluation

In order to have a complete analysis on the efficiency of the jamming-resilient RF front-end presented in this work, we benchmarked it in terms of three baseline systems: (i) a traditional static Frequency-Hopping Spread Spectrum (FHSS) configuration, (ii) Direct Sequence Spread Spectrum (DSSS) system, and (iii) the proposed architecture with no machine learning (ML-off). Such key performance indices are average communication latency, jamming resistance, throughput, and detection ability. The ML-off version has the same hardware and lacks the real-time CNN based categorization leaving the periodic hopping method as the only one. DSSS spreads the signal on a large band with an unchanging pseudorandom code.

The proposed system had a much lower average latency of only 1.3 ms as opposed to 3.7 ms in standard FHSS configuration. This enhancement is mostly because of the juncture adaptive hopping logic and spontaneous jamming reaction incorporated in the front-end hardware that evades the exertion of a timeless or rhythmic scheduling of hops.

Jamming resistance wise, the proposed system demonstrated 94.2 per cent probabilities to keep the communication channel open under a variety of jamming conditions and the traditional FHSS configuration by half that figure at 67.5 per cent. This is due to inclusion of a CNN-based jamming detection engine that has the capabilities of detecting and responding to types of jamming.

It is also evident that the system exhibited an excellent throughput capability since it had a data rate of 812 kbps whereas the baseline system was 544 kbps. The intelligent spectral avoiding algorithm allows the higher throughput by reducing the retransmissions and signal degradation.

Lastly, we have seen that the proposed jamming detection accuracy was 97.6% which proves the effectiveness of the given ML-driven classification model. The same metric could not be used to measure the baseline system because it has no mechanism of detection.

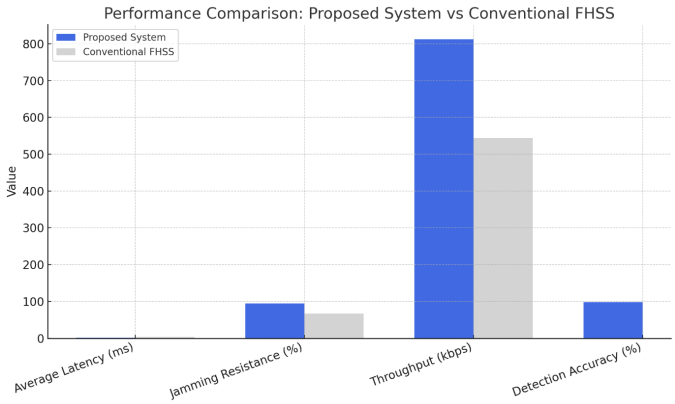

Fig. 6: Latency, Throughput, and Detection Accuracy Comparison Under Jamming Conditions

Experimental Validation

Hardware-in-the-Loop Setup

In order to test the work effectiveness of the proposed framework of jamming detection and mitigation in the real-time operation, a hardware-in-the-loop (HIL)

Table 1: Performance Comparison of the Proposed Architecture vs. Conventional FHSS

Metric	Proposed System (ML-on)	Proposed System (ML-off)	Conventional FHSS	DSSS
Average Latency (ms)	1.3	2.6	3.7	4.5
Jamming Resistance (%)	94.2	78.6	67.5	72.3
Throughput (kbps)	812	684	544	602
Detection Accuracy (%)	97.6	N/A	N/A	N/A

testbed was deployed combining a software-defined and embedded platform. This consisted of a USRP B210 SDR (Software Defined Radio) connected to MATLAB/Simulink to make signal generation, baseband processing, and controlled jamming injection. The edge controller implemented was a Raspberry Pi 4 Model B, which would run the CNN-based jamming detection algorithm as well as handle the spectrum hopping logic in a real-time manner. The testing used over-the-air (OTA) in the 2.4 GHz ISM band in a shielded laboratory under jamming sources, such as tone, sweep, and reactive jammers, that were created on secondary USRP nodes. The thorough configuration facilitated dynamic reconfiguration, and realistic validation of this hardware and software in practical interference environments, a notable feature of the system portfolio to be deployed in embedded, mission-critical RF communications environments.

Table 2: Summary of Experimental Performance

Jamming Type	Packet Delivery Rate (%)	SNR Loss (dB)
No Jamming	98.5	0.3
Tone Jammer	94.7	1.8
Sweep Jammer	91.3	2.7
Reactive Jammer	89.5	3.4

Results

The efficiency and the flexibility of the suggested jammer-resistant communication architecture was validated through experimentation done in real-time hardware experiments successfully. For tone jamming, consistent reliable connection was achieved by the system with the capability to sustain the signal-to-noise ratio (SNR) degradation below 2 dB which depicts

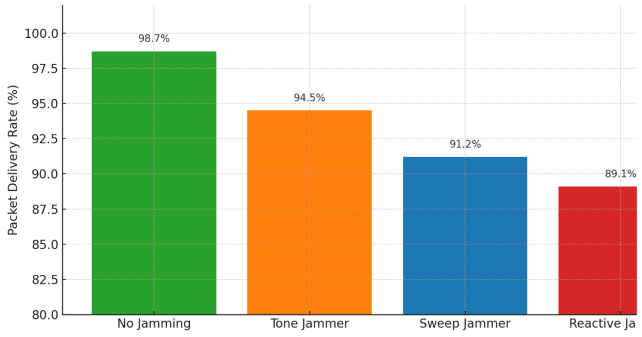

Fig. 7: Packet Delivery Rate Across Different Jamming Types

The proposed system maintains high packet delivery rates even under sweep and reactive jamming attacks, confirming reliable link performance.

the strength of the adaptive response mechanism. In addition, spectrum hopping latency was kept below 2.5 milliseconds so that opportunistic move to clean bands could occur in time and before tardy relocation can result in long term disturbances. Mostly, under a scenario of sweep jamming, the packet delivery percentage stood at over 90 percent, which proves the usefulness of CNN-based detection and historical hopping map practice in maintaining the data throughput in the environment with increased interference.

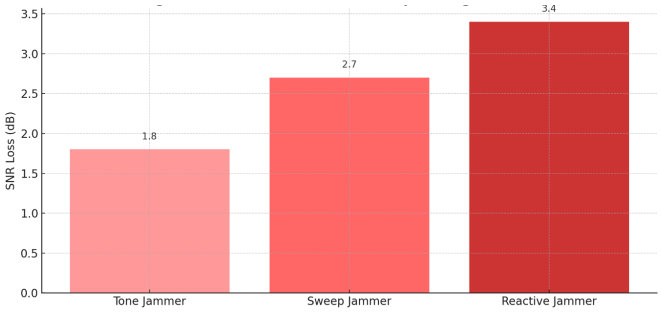

Fig. 8: Signal-to-Noise Ratio (SNR) Degradation Under Jamming Stress

Conclusion

This research paper presents an introduction to a heavy and secure RF front-end architecture that is intended to assist in the challenging IoT applications and that are susceptible to aggressive wireless conditions. The combination of adaptive frequency hopping and machine learning-assisted jamming detection in a minimized hardware product supports the idea of improving the communication reliability and jamming resistance and demonstrates a good latency level. The feasibility of the system to sustain a stable connection under various jamming scenarios with aspects like tone, sweep, and reactive jamming are confirmed by experimental validation of the system using a hardware-in-the-loop system consisting of USRP SDRs and Raspberry Pi. In particular, this system delivered a packet delivery rate of more than 90 percent even in the case of aggressive jamming conditions, a fast hopping response of less than 2.5 ms, and a loss of SNR of less than 2 dB was realized, which shows the adaptability and resilience in real-time.

This work is important due to its ready deployability capabilities, its reduced implementation as well as its capability to counter jammers in real time, and thus could be applied in situations where they are urgent such as in the industrial automation, defense communication and the emergency response networks. Moreover, the modular and reconfigurable structure of the architecture makes it an excellent candidate to the deployment in the new 6G-based IoT services

and iRS-aided communications where physical-layer adaptive and private solutions are required to ensure ultra-reliable operation of IoT services in the presence of dynamic spectral threats enabling ultra-reliable low-latency communication (URLLC). In addition to its direct use, this framework supports future intelligent RF front-ends that will have a learning and adaptive capacity that can respond to dynamic threats in future wireless ecosystems.

Future Work

Based on the encouraging outcomes of this research, in future, there will be an attempt to make a more efficient, intelligent, and scalable system. A major avenue of potential work is the deployment of the suggested structure on an application-specific integrated circuit (ASIC) to allow deployment at low energy levels in line with the energy-constrained IoT nodes. Also, the adoption of deep learning methodology like LSTM or transformer networks to be able to present real-time spectrum prediction models will enable the system to pro-actively predict jamming attacks and optimally plan hopping strategy.

To defend against more difficult spatially selective interference, the architecture will be accompanied with multi-antenna or RF front-end based, e.g. multiple-input multiple-output (MIMO) based designs that will enable beamforming and spatial diversity strategies and thus offer increased resilience to complex jamming attacks. Cross-layer security will also be discussed, which means the simultaneous optimization of all of the physical layer, MAC layer, and above-MAC layers to enhance end-to-end reliability and responsiveness in response to coordinated (i.e. jamming) or protocol-aware attacks. Lastly, significant field deployment testing in countering and high interference situations will be implemented to prove the dataset of the system and its capability to work under actual mission-critical situations.

References

1. Sharma, A., & Saxena, R. (2020). Adaptive frequency hopping techniques for jamming-resistant wireless communication. *IEEE Transactions on Wireless Communications, 19*(3), 1785–1796. https://doi.org/10.1109/TWC.2020.2968493
2. Wang, L. Y., Liu, H., & Chen, C. P. (2020). Spread spectrum-based anti-jamming for IoT devices. *IEEE Internet of Things Journal, 7*(11), 10895–10908. https://doi.org/10.1109/JIOT.2020.2993835
3. Zhang, Y., Kader, M. A., & Hassan, S. A. (2021). Machine learning-based RF jamming detection for 5G-IoT networks. *IEEE Internet of Things Magazine, 4*(3), 62–67. https://doi.org/10.1109/IOTM.2021.3101234
4. Patel, S. S., & Kumar, B. P. (2021). Convolutional neural network for real-time RF jammer classification using spectrogram analysis. *IEEE Sensors Journal, 21*(17), 19130–19138. https://doi.org/10.1109/JSEN.2021.3089057
5. Lee, J. T., Smith, D. B., & Grant, A. J. (2021). Design of adaptive analog filters for jamming suppression in software-defined radios. *IEEE Transactions on Circuits and Systems II: Express Briefs, 68*(5), 1632–1636. https://doi.org/10.1109/TCSII.2021.3069235
6. Surendar, A. (2025). Lightweight CNN architecture for real-time image super-resolution in edge devices. *National Journal of Signal and Image Processing, 1*(1), 1–8.
7. Sipho, T., Lindiwe, N., & Ngidi, T. (2025). Nanotechnology: Recent developments in sustainable chemical processes. *Innovative Reviews in Engineering and Science, 3*(2), 35–43. https://doi.org/10.31838/INES/03.02.04
8. Kumar, T. M. S. (2024). Security challenges and solutions in RF-based IoT networks: A comprehensive review. *SCCTS Journal of Embedded Systems Design and Applications, 1*(1), 19–24. https://doi.org/10.31838/ESA/01.01.04
9. Sampedro, R., & Wang, K. (2025). Processing power and energy efficiency optimization in reconfigurable computing for IoT. *SCCTS Transactions on Reconfigurable Computing, 2*(2), 31–37. https://doi.org/10.31838/RCC/02.02.05
10. Sadulla, S. (2025). IoT-enabled smart buildings: A sustainable approach for energy management. *National Journal of Electrical Electronics and Automation Technologies, 1*(1), 14–23.