

Low-Cost Embedded Hardware for RF Jamming Detection in IIoT Environments

Patrícia R. Araújo¹, Décio R. M. Faria¹, Raul G. O. Bortoloto¹,
Raphael C. S. Machado², Otávio S. M. Gomes¹

¹Systems Engineering and Information Technology Institute
Federal University of Itajuba (UNIFEI)
Av. BPS, 1303 – Building I – 37500-903 – Itajuba, MG – Brazil

²Clavis Information Security
Flamengo Beach, 66 – Building B – 22210-030 – Rio de Janeiro, RJ – Brazil

{patricia.araujo, deciorennno, d2020012183}@unifei.edu.br,
raphael.machado@clavis.com.br, otavio.gomes@unifei.edu.br

Abstract. *RF jamming attacks compromise the availability of wireless industrial systems regardless of the authentication and encryption state, representing a cyberattack vector capable of inducing operational failures that are difficult to detect. Existing approaches present limitations in complexity, cost, or integration that hinder their adoption in resource-constrained embedded systems. In this context, this work presents a low-cost embedded device for jamming detection, implemented for systems operating at 13.56 MHz or 433 MHz, with a focus on IIoT environments. The prototype was validated on a test bench with a maximum detection latency of 10.24 ms, enabling its use in environments with restricted operational budgets.*

1. Introduction

Wireless systems are critical components of modern industrial environments [National Institute of Standards and Technology (NIST)], and cyberattacks against these technologies remain relevant in Industrial Internet of Things (IIoT) ecosystems [Anthi et al. 2024, Araújo et al. 2026, Uribe et al. 2022]. Although mechanisms such as encryption, digital signatures, and rolling code protect confidentiality and integrity, two of the three pillars of the CIA triad [ISO/IEC 2018], the availability of the radiofrequency (RF) channel remains exposed to interference at the physical layer. In particular, RF jamming attacks interfere with the physical transmission medium, suppressing communication without triggering any cryptographic or authentication mechanism, as shown by vulnerabilities cataloged in CVE-2021-40171 [National Vulnerability Database (NVD) 2021] and CVE-2025-65553 [National Vulnerability Database (NVD) 2026] and experimentally demonstrated in LoRaWAN networks [Perković et al. 2021, Sabic et al. 2025]. In industrial environments, bands such as 13.56 MHz, used in HF RFID for asset tracking and access control, and 433 MHz, present in wireless sensors and telemetry systems, are representative examples of infrastructures exposed to this form of interference.

This attack vector is aggravated by the accessibility of the means required to execute it, since interference devices can be built using low-cost hardware and software-defined radio (SDR) [Perković et al. 2021, Sabic et al. 2025, Pirayesh and Zeng 2022,

Uribe et al. 2022], making this form of interference feasible even for adversaries with limited resources. In industrial environments, this threat becomes critical because suppression of the RF channel can interrupt telemetry, compromise remote actuation, and cause immediate operational consequences [Anthi et al. 2024, Ma et al. 2023]. In addition to the difficulty of detection, firmware or protocol modifications in systems under continuous operation require formal validation procedures and planned maintenance windows [Mugarza et al. 2020].

Despite the operational relevance of this threat, existing approaches for jamming detection present practical limitations in industrial embedded devices, namely, machine learning-based methods require computational capacity and training data beyond what Internet of Things (IoT) devices typically provide [Zahra et al. 2023, Lee et al. 2023], and even embedded hardware implementations require extensive datasets for training [Sormayli et al. 2025]; protocol-level strategies demand modifications to the communication stack [Letafati et al. 2020, Ahmar et al. 2023]; solutions based on additional infrastructure increase deployment cost and complexity [Bhamidipati and Gao 2019]; low-cost approaches based on signal level, such as [Mittal and Shrivastava 2022], have been validated only in simulation and at different frequencies; and solutions that depend on dedicated external receivers [Kazim et al. 2025, Sormayli et al. 2025] limit their adoption as independent diagnostic instruments in the field.

In the absence of dedicated diagnostic tools, failures caused by jamming may be confused with hardware defects, generating costly and unnecessary corrective maintenance cycles, a limitation that motivated the development of the proposed solution. In this context, this work presents a low-cost embedded device for RF jamming detection in IIoT environments, implemented with deterministic bare-metal C firmware in the 13.56 MHz or 433 MHz bands, using Commercial Off-The-Shelf (COTS) components and an architecture adaptable to other bands of industrial interest. The threat model considered in this initial prototype comprises abrupt interference that produces a high channel-occupancy level during the observation window. This model was selected to enable the validation of a low-cost deterministic diagnostic architecture. More sophisticated scenarios, including intermittent, low-duty-cycle, or randomly pulsed jamming, are outside the current scope and will be investigated in future work. This work was developed within the CyberOT Project, a collaboration between UNIFEI and Clavis Information Security, combining academic research and industry expertise in applied cybersecurity.

2. Architecture Overview

The device proposed in this work monitors RF channel availability at the physical layer independently of the main communication chain. Instead of inspecting payloads or protocol exchanges, signal levels are continuously analyzed within predefined observation windows and compared with a threshold calibrated for the operating environment. The architecture consists of four main stages, signal acquisition, analog conditioning, signal level extraction, and deterministic classification, as illustrated in Figure 1.

2.1. Signal Acquisition

The device antenna captures RF signals in the 13.56 MHz or 433 MHz bands, which are frequencies commonly found in wireless communication devices in IIoT environments.

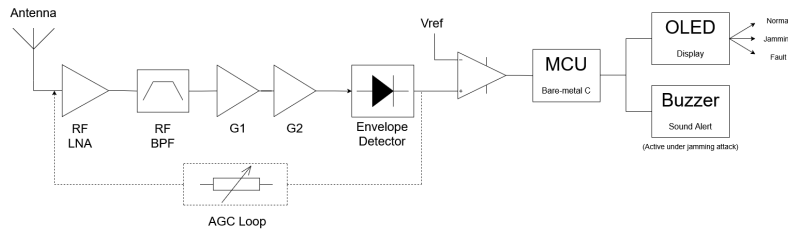


Figure 1. Block diagram of low-cost embedded hardware.

The captured signal is forwarded to a low-noise amplifier (LNA) based on a BF998 dual-gate MOSFET transistor, whose function is to increase the level of the received signal before processing by the subsequent stages. Because it is designed to introduce minimal noise during amplification, the LNA ensures that low-power signals are amplified without loss of quality, preserving the detection capability of the device even in industrial environments with multiple sources of interference.

2.2. Analog Conditioning

After the initial amplification, the captured signal is analogically conditioned to isolate the frequency range of interest and adjust its amplitude for the subsequent stages. For this purpose, discrete LC bandpass filters centered at the operating frequencies are used to attenuate components outside the monitored bands and reduce the influence of noise and emissions from other radiofrequency sources present in the environment. Then, the amplitude is adjusted through two cascaded BF518 transistor stages to avoid both insufficient levels for detection and excessive amplitudes that could saturate the circuit, ensuring that the analyzed variations reflect the behavior of the channel rather than distortions introduced by the acquisition chain.

The stage also integrates an analog automatic gain control (AGC) loop implemented with a 100 k Ω potentiometer for threshold adjustment, which feeds back the input amplifier from the output voltage of the envelope detector, keeping the signal level stable under natural variations in channel power. This mechanism operates entirely in hardware, without software intervention, and is designed to compensate for gradual power fluctuations caused by distance, obstruction, or reflections in the environment. The loop time constant ($\tau \approx 3.3ms$), adjusted for this variation profile, does not track abrupt high-power events caused by intentional interference, so these events saturate the loop and raise the output level above the calibrated threshold, being detected by the classification stage.

2.3. Signal Extraction

The signal extraction stage uses an envelope detector, a circuit that extracts the amplitude variation of an RF signal, implemented by means of a signal diode detector (1N4148W) that rectifies the amplified signal by eliminating the negative alternations. An RC filter smooths the rectified pulses into a continuous voltage proportional to the signal intensity in the monitored band. This voltage is then fed into an LM358 comparator, which converts the analog envelope level into a logic-level digital signal, high when the carrier is present and low otherwise, forwarded to the microcontroller GPIO pin.

2.4. Digital Classification

Digital classification is performed by an STM32F103C8T6 microcontroller that monitors the comparator output through a GPIO pin, eliminating the need for an analog-to-digital converter. The architecture is compatible with other low-cost MCUs, such as the PIC family, provided that the timing parameters are recalculated.

The sampling rate of 100 kHz was defined according to the Nyquist-Shannon criterion, under which directly sampling the RF carriers would require 27.12 MHz and 866 MHz for 13.56 MHz and 433 MHz, respectively, rates that are impractical for low-cost MCUs. Since the external demodulator already performs carrier detection, the maximum relevant frequency becomes the data rate of the monitored protocol. For OOK signals at 433 MHz and 10 kbps, the output varies at a maximum of 10 kHz, requiring a minimum sampling rate of 20 kHz. For 13.56 MHz, transitions occur on the millisecond scale, imposing even lower requirements. The adopted rate operates with a $5\times$ margin above what is required for both bands.

With this rate, the samples are grouped into 1024-point windows (10.24 ms). The firmware calculates the percentage of samples at a high level and classifies the channel based on configurable thresholds. Values above the upper threshold indicate *Jamming*; values below the lower threshold indicate *Fault*; and values between the two correspond to *Normal*, as illustrated in Figure 2. This window was sized to avoid false alarms caused by legitimate preambles, since a 100-byte preamble represents 78% of the window, below the upper threshold, and is therefore classified as *Normal*.

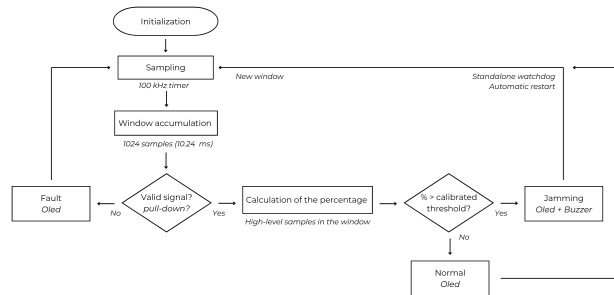


Figure 2. Flowchart of the jamming detection method.

In addition to the classification criterion, the firmware was developed in bare-metal C, without an operating system, RTOS, HAL layer, or external libraries, except for minimal inline assembly used only for Cortex-M interrupt control and low-power waiting. The circuit adopts a *pull-down* configuration at the microcontroller input, ensuring *fail-safe* behavior, so that in the absence of a valid signal the system assumes *Fault* rather than *Normal*. An independent watchdog ensures automatic reset in case of lockup. The complete firmware source code is publicly available at https://github.com/patyrodriguesar/rf_dual_band-firmware.

2.5. Integration Interface and Operational Scope

The device operates autonomously, powered by battery, without relying on external infrastructure. The operational state is indicated in real time through an SSD1306 OLED display (I2C) and audible alert under three conditions, *Normal*, *Jamming*, and *Fault*, allowing immediate diagnosis without specialized training. Regarding the operating modes,

the device can be used for field inspection or fixed monitoring, without modifications to the monitored system. The use of COTS components enables deployment in environments with restricted budgets, and extension to other bands requires redesign of the RF front-end and recalculation of the AGC loop time constants. The total bill of materials for the prototype remains below USD 15, consistent with the low-cost deployment objective. The released artifacts correspond to the current prototype stage. Accordingly, the circuit schematic is not included, as the hardware design remains under validation through extended jamming test scenarios and IEC 62443-oriented assessment [ISA/IEC 2007].

3. Hardware Validation and Results

Preliminary validation experiments were conducted using a Keysight 33500B waveform generator and a Rohde & Schwarz RTB2002 oscilloscope, as illustrated in Figure 3. The classification thresholds are configurable in firmware and, for these experiments, the Jamming threshold was set to 85%, a value compatible with the operating range of the available generator. Since the STM32F103C8T6 operates exclusively on the digital output of the comparator stage, the function generator replicates the exact signal seen by the microcontroller under real RF conditions. This approach validates the classification criterion, firmware behavior, and detection latency independently of the RF front-end, whose validation with actual RF signals at 13.56 MHz or 433 MHz using an MG3710A vector signal generator (Anritsu), following the methodology of [Araújo et al. 2025], is planned as future work.

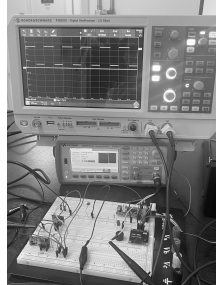


Figure 3. Experimental Setup.

The three operational states were validated on a test bench, as illustrated in Figure 4. The *Normal* state occurs when the channel exhibits activity compatible with legitimate communication; the *Jamming* state, when the percentage of samples at a high level exceeds the configured threshold, with simultaneous activation of the display and an indicator LED used in place of the buzzer for visual validation; and the *Fault* state, when the input signal is absent or invalid.

Classification was validated across multiple duty cycle values. Signals at 95%, 90%, 87%, 86% and 85%, all exceeding the configured threshold, were consistently detected as *Jamming* with immediate activation of the indicator LED. Signals at 30%, 40%, 55%, 70%, and 84% were correctly classified as *Normal*. All tested cases produced the expected classification, yielding a detection rate of 100% across the 10 evaluated test points. Figure 5 presents the oscilloscope captures for both scenarios, and the maximum detection latency, analytically bounded, corresponds to the duration of one complete window, given by $1024 \times (1/100 \text{ kHz}) = 10.24 \text{ ms}$.

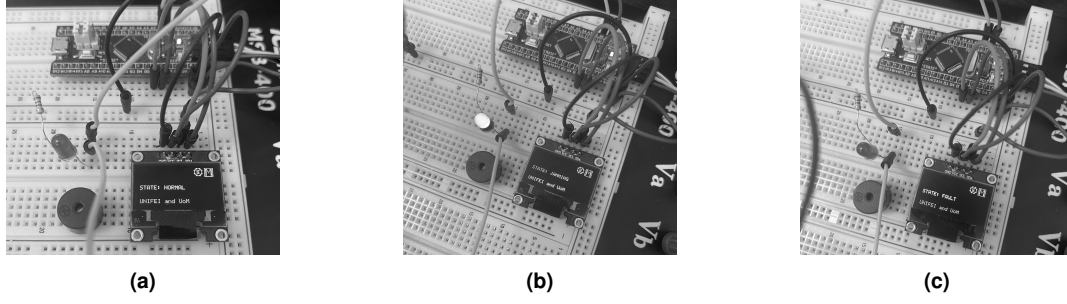


Figure 4. Operational states: (a) *Normal*, (b) *Jamming* and (c) *Fault*.

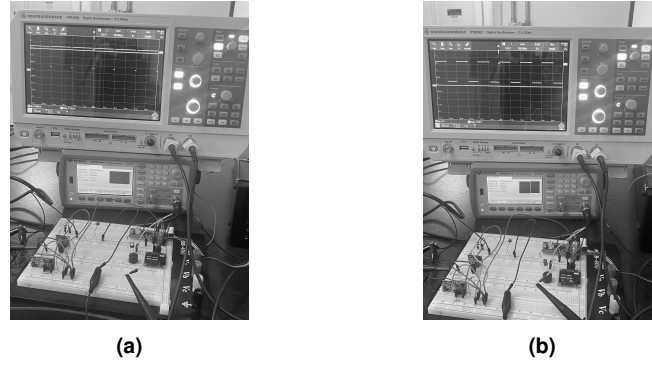


Figure 5. Duty cycle: (a) 95% at *Jamming* and (b) 55% at *Normal*.

These results demonstrate that the proposed deterministic classification method reliably distinguishes Normal and Jamming conditions for the evaluated duty-cycle values, while maintaining a bounded detection latency of 10.24 ms. The experiments also confirm the correct integration between the firmware, visual indication, and alarm output. However, the present validation is limited to controlled signals applied to the comparator output, and complete validation of the RF front-end with actual 13.56 MHz and 433 MHz signals remains future work.

Table 1 presents a qualitative comparison among works related to jamming detection in embedded devices. Quantitative metrics are presented for reference only, as the works operate in different frequency ranges and application domains.

Table 1. Qualitative comparison of related works.

Description	Kazim et al. (2025)	Sormayli et al. (2025)	Mittal and Shrivastava (2022)	This work
Frequency	1575.42 MHz (GPS L1)	1575.42 MHz (GPS L1) / 1602 MHz (GLONASS L1)	2.4 GHz	13.56 MHz / 433 MHz
Architecture	Software AGC	Software AGC	No AGC	Hardware AGC
Approach	Deterministic	Machine Learning + Deep Learning	Deterministic	Deterministic
Training Data	Not required	51,315 samples	Not required	Not required
Complexity	High	High	Low	Low
Detection Rate	100% (AGC) / 76.5% (CNO)	99.97% (desktop) / 98% (embedded)	N/A (simulation)	100% (embedded)
Cost	High	High	Low	Low
Jamming Type	Chirp	Suppression + Deception	Continuous	Continuous
Validation	Physical prototype	Physical prototype	Simulation only	Physical prototype
Detector	AsteRx SBi3 receiver + Computer	Ublox-M8T receiver + STM32H7 + Computer	Passive RSSI circuit	Dedicated embedded hardware
Autonomy	Host-dependent	Host-dependent	On-chip integration	Battery-powered
Field Use	Fixed	Fixed	Fixed	Portable or Fixed
Context	Railway	GNSS Navigation	Generic IoT	IIoT

The analysis reveals three groups of solutions. [Kazim et al. 2025] and [Sormayli et al. 2025] present high cost and dependence on external receivers, limiting

their adoption as independent field diagnostic instruments. [Sormayli et al. 2025] further requires 51,315 training samples, making its application infeasible without historical data. [Mittal and Shrivastava 2022] propose a low-cost solution with a deterministic approach, however validated only in simulation. The proposed device shares with Mittal the low cost and deterministic approach, but is validated on a physical prototype with COTS components and autonomous field operation.

4. Conclusion

This work presented a low-cost embedded device for RF jamming detection in IIoT environments, implemented as bare-metal firmware for the 13.56 MHz or 433 MHz bands using COTS components, requiring no training data and no modification of the monitored systems. The solution was validated on a physical prototype with a maximum detection latency of 10.24 ms, operating autonomously with immediate field diagnosis. Although the device was developed for intentional and abrupt interference, sophisticated jamming devices with random pulse generation that partially block communication may not be detected, constituting a limitation of the adopted threat model. Future work includes the fabrication of the printed circuit board with final RF front-end testing, formal firmware verification via model checking to ensure the absence of false positives and reliable real-time detection, mitigation of the identified limitation, extension to other industrially relevant frequency bands, and compliance evaluation with IEC 62443.

5. Acknowledgments

The authors would like to thank the Federal University of Itajubá (UNIFEI), Clavis Information Security (FINEP/Plat-Ciber) for their collaboration and financial support within the scope of the CyberOT Project, and the LabTel, LAIoT, u.AI, and FrontTIERS HackLab laboratories for their technical support.

References

- Ahmar, A. U. H., Aras, E., Nguyen, T. D., Michiels, S., Joosen, W., and Hughes, D. (2023). Design of a robust mac protocol for lora. *ACM Transactions on Internet of Things*, 4(1):1–25.
- Anthi, E., Williams, L., Ieropoulos, V., and Spyridopoulos, T. (2024). Investigating radio frequency vulnerabilities in the internet of things (iot). *IoT*, 5(2):356–380.
- Araújo, P. R., Bortoloto, R. G. O., Faria, D. R. M., and Gomes, O. S. M. (2025). Rf cyber range: Building communication scenarios using software-defined radio for radio frequency vulnerability analysis. In *Anais do XXV Simpósio Brasileiro de Cibersegurança (SBSeg)*, pages 757–773.
- Araújo, P. R., Rezende, J. A. M., Faria, D. R. d. M., and Gomes, O. d. S. (2026). Cybersecurity in radio frequency technologies: A scientometric and systematic review with implications for iot and wireless applications. *Sensors*, 26(2):747.
- Bhamidipati, S. and Gao, G. X. (2019). Locating multiple gps jammers using networked uavs. *IEEE Internet of Things Journal*, 6(2):1816–1828.
- ISA/IEC (2007). ISA/IEC 62443 — security for industrial automation and control systems.

- ISO/IEC (2018). ISO/IEC 27000:2018 — information security management systems.
- Kazim, S. A., Darwich, A., and Marais, J. (2025). GNSS jamming detection with automatic gain control (AGC) and carrier-to-noise ratio density (CNO) observables from a COTS receiver. In *7th SmartRacon Scientific Seminar*.
- Lee, S. J., Lee, Y. R., Jeon, S. E., and Lee, I. G. (2023). Machine learning-based jamming attack classification and effective defense technique. *Computers & Security*, 128:103169.
- Letafati, M., Kuhestani, A., Behroozi, H., and Ng, D. W. K. (2020). Jamming-resilient frequency hopping-aided secure communication for internet-of-things in the presence of an untrusted relay. *IEEE Transactions on Wireless Communications*, 19(10):6771–6785.
- Ma, S., Wang, H., Zhu, L., and Zhang, Q. (2023). Joint security and resilience control in iiot-based virtual control train sets under jamming attacks. *IEEE Transactions on Vehicular Technology*, 72(9):11196–11212.
- Mittal, A. and Shrivastava, A. (2022). Detecting continuous jamming attack using ultra-low power RSSI circuit. In *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 49–52.
- Mugarza, I., Flores, J. L., and Montero, J. L. (2020). Security issues and software updates management in the industrial internet of things (iiot) era. *Sensors*, 20(24).
- National Institute of Standards and Technology (NIST). Industrial wireless systems. NIST Programs and Projects. Accessed 2026-04-12.
- National Vulnerability Database (NVD) (2021). CVE-2021-40171 detail. National Vulnerability Database (NVD). Accessed 2026-04-8.
- National Vulnerability Database (NVD) (2026). CVE-2025-65553 detail. National Vulnerability Database (NVD). Accessed 2026-04-8.
- Perković, T., Rudeš, H., Damjanović, S., and Nakić, A. (2021). Low-cost implementation of reactive jammer on lorawan network. *Electronics*, 10(7):864.
- Pirayesh, H. and Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys Tutorials*, 24:767–809.
- Sabic, J., Perkovic, T., Begusic, D., and Solic, P. (2025). Practical realization of reactive jamming attack on long-range wide-area network. *Sensors*, 25:2383.
- Sormayli, J., Darvishi, M., Zarrinnegar, K., and Mosavi, M. R. (2025). Real-time jamming detection using windowing and hybrid machine learning models for pre-saturation alerts. *Scientific Reports*, 15:24748.
- Uribe, J. d. J. R., Guillén, E. P., and Cardoso, L. S. (2022). A technical review of wireless security for the internet of things: Software defined radio perspective. *Journal of King Saud University - Computer and Information Sciences*, 34(7):4122–4134.
- Zahra, F. T., Bostanci, Y. S., and Soy Turk, M. (2023). Real-time jamming detection in wireless iot networks. *IEEE Access*, 11:70425–70442.