RF Cyber Range: Building Communication Scenarios Using Software-Defined Radio for Radio Frequency Vulnerability Analysis

Patrícia R. Araújo[1], **Raul G. O. Bortoloto**[1], **Décio R. M. Faria**[1], **Otávio S. M. Gomes**[1]

[1]Systems Engineering and Information Technology Institute
Federal University of Itajubá (UNIFEI)
Av. BPS, 1303 – Building I – 37.500-903 – Itajubá – MG – Brazil

{patricia.araujo,d2020012183,deciorenno,otavio.gomes}@unifei.edu.br

Abstract. *The 433 MHz frequency band is widely used by low-cost wireless devices such as sensors and alarm systems, but it often lacks robust security mechanisms. This work proposes the construction of communication scenarios for vulnerability analysis in RF devices using software-defined radios (SDR). The methodology combines scientometric analysis, a survey of vulnerabilities from CVE databases, and both simulated and practical experiments using GNU Radio and RTL-SDR. The results demonstrate the feasibility of attacks such as jamming and replay, highlighting the risks associated with the absence of authentication and encryption in these devices. Results highlight the need for RF security and validate SDR for vulnerability testing.*

1. Introduction

Radio frequency (RF) communication plays a key role in wireless connectivity, particularly in Internet of Things (IoT) devices, encompassing applications in home automation, industrial systems, and electronic security. Among the commonly used frequency bands, the 433 MHz band, part of the UHF range and the Industrial, Scientific, and Medical (ISM) spectrum, stands out. This band is widely adopted by low-power devices such as remote controls, sensors, alarms, and building automation equipment [Kumbhar 2017, ITU 2010], operating without licensing requirements in many countries, including Brazil, in accordance with ANATEL [Anatel 2025] and ITU-R regulations [ITU 2025].

Despite its popularity and flexibility, devices operating in the 433 MHz band often lack advanced security mechanisms, such as encryption, authentication, or interference detection. This limitation makes them vulnerable to attacks such as jamming, replay, and spoofing, which can be carried out using accessible tools such as software-defined radios (SDRs). These attacks compromise the integrity and availability of the systems, with potential impact on both domestic environments and critical applications.

In response to this scenario, this work presents RF Cyber Range, a novel framework that builds experimental communication scenarios using SDR to analyze vulnerabilities in the 433 MHz band. The methodology integrates scientometric review, CVE analysis, and both simulated and real-world tests with GNU Radio and RTL-SDR. It identifies exploitable attack vectors, validates documented threats, and introduces reproducible scenarios to support practical RF security assessments.

2. Background

The 433 MHz band is widely used in low-cost, unlicensed wireless applications such as sensors, alarms, remote controls, and automation systems. However, its open nature makes these devices highly vulnerable to cyberattacks, especially Denial-of-Service (DoS). The most common method is jamming, which disrupts communication by interfering with the frequency [Lau et al. 2000]. Other attacks target energy constraints, such as battery drain and sleep deprivation, keeping devices active until power is depleted [Abdul-Ghani and Konstantas 2019].

Recent studies confirm that 433 MHz devices are highly vulnerable to jamming and replay attacks, which can be executed remotely and compromise critical systems [Allen et al. 2024, Mykhaylova et al. 2024, Muñoz et al. 2023, Najath et al. 2022]. As noted by [Anthi et al. 2024], the absence of authentication, encryption, and dedicated channels facilitates these intrusions, especially with accessible tools like software-defined radios. Although mitigation measures such as more robust protocols and intrusion detection systems exist, their adoption in this context remains limited.

2.1. Software-Defined Radio

Radio frequency communication is based on the transmission of electromagnetic waves, which are synchronized variations of electric and magnetic fields over time. A fundamental characteristic of these waves is the ability for multiple signals to occupy the same physical space, as long as they are at different frequencies. This property allows electronic circuits to separate signals, enabling the coexistence of services like FM radio, television, mobile networks, and IoT within the same electromagnetic spectrum [Ribeiro 2008].

In radio communication systems, the carrier wave is a high-frequency periodic signal onto which information (such as voice, data, or video) is inserted through modulation, a process that alters certain parameters of the wave, such as amplitude, frequency, or phase. Mathematically, electromagnetic wave at a single frequency can be described as:

$$e_0(t) = E_0.cos(2.\pi.f_0.t + \phi)$$

Where:

E_0 is the peak voltage of the electromagnetic wave,

f_0 is the frequency of the electromagnetic wave,

ϕ is the phase angle of the wave.

This signal is referred to as a carrier. The insertion of an information signal, whether analog or digital, is achieved by varying the amplitude, frequency, or phase of the carrier signal. Transmissions that vary the amplitude to convey information are known as Amplitude Modulation (AM), while others are categorized as Frequency Modulation (FM) or Phase Modulation (PM). In digital transmissions, many modulation schemes convey binary data (zeros and ones) through simultaneous variations in amplitude and phase (or frequency), enabling combinations that allow the transmission of multiple bits in a single signal variation.

A signal modulated in both amplitude and frequency simultaneously can be described by:

$$m(t) = a(t).cos(2.\pi.f_0.t + \phi(t))$$

$$m(t) = a(t).e^{j(2.\pi.f_0.t+\phi(t))} \quad \text{or} \quad m(t) = a(t).e^{j.\phi(t)}.e^{j.2.\pi.f_0(t)}$$

Clearly, the modulated signal is formed by the carrier signal multiplied by the modulating signal (the information), mathematically described as follows:

$$m'(t) = a(t).e^{j.\phi(t)}$$

From this mathematical model, the modulating signal can be rewritten as follows:

$$m'(t) = i(t) + j.q(t)$$

In other words, the modulating signal can be obtained by combining two signals with a 90º phase shift, known as I (in-phase) and Q (quadrature) components. It is important to note that, by multiplying this signal by the carrier wave, the modulated radio signal can be obtained.

$$m(t) = i(t).cos(2.\pi.f_o.t) - q(t).sin(2.\pi.f_o.t)]$$

The resulting signal m(t) can represent any type of modulation, AM, PM, or any combination thereof. This model is currently used by most modern transmitters and receivers. The I and Q signals are obtained through circuits that introduce a phase delay. In a modern receiver, the analog I and Q signals are converted into digital signals by Analog-to-Digital Converters (ADCs), which perform the sampling and quantization processes. In a software-defined radio (SDR), signal filtering and demodulation are carried out through mathematical processes that emulate the ideal behavior of physical components (see Figure 1).

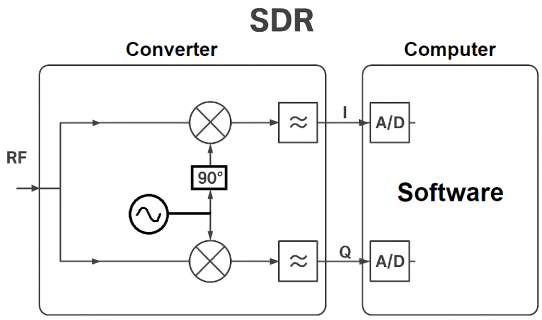

Figure 1. Internal diagram of a Software-Defined Radio device.

A complex signal can be understood as a signal composed of a very large number, or even an infinite number, of component signals. The Fourier Transform is the most commonly used mathematical tool by engineers to analyze the behavior of a signal in the frequency domain, that is, its frequency spectrum.

$$F(\omega) = \int_{-\infty}^{\infty} f(t).e^{-j.\omega.t}dt$$

When a signal is converted into a digital signal, a different mathematical process must be applied, since we are now working with a sequence of values resulting from the analog-to-digital conversion. In this case, a variation of the Fourier Transform is used, called the Discrete Fourier Transform (DFT), defined as follows:

$$X(k) = \frac{1}{N} \sum_{N=0}^{N-1} x(n).[cos(2.\pi.n.\frac{k}{N}) - j.sin(2.\pi.n.\frac{k}{N})]$$

With this feature, a software-defined radio is not only capable of demodulating the signal, but also of obtaining its frequency spectrum, as illustrated in Figure 2.

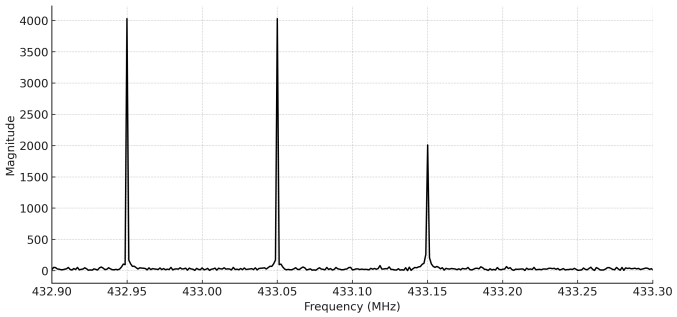

Figure 2. Example of a frequency spectrum.

3. Methodology

The methodology was structured into four stages: (i) scientometric review to map the scientific literature on cybersecurity in the 433 MHz band; (ii) analysis of selected articles to extract key findings; (iii) investigation of CVE-documented vulnerabilities affecting 433 MHz devices; and (iv) construction of practical scenarios, including GNU Radio simulations and laboratory-based signal interference experiments.

3.1. Scientometric Analysis

Research articles on cybersecurity in 433 MHz RF devices were retrieved from Scopus and Web of Science [Scopus 2025, ISI Web of Science 2025], accessed on March 18, 2025. Both databases are internationally recognized for indexing peer-reviewed literature [Zhu and Liu 2020]. Accordingly, the scientometric analysis aimed to identify studies on vulnerabilities, attack techniques, and protection strategies. The search and selection process is summarized in the PRISMA flowchart (Figure 3) [Page et al. 2021].

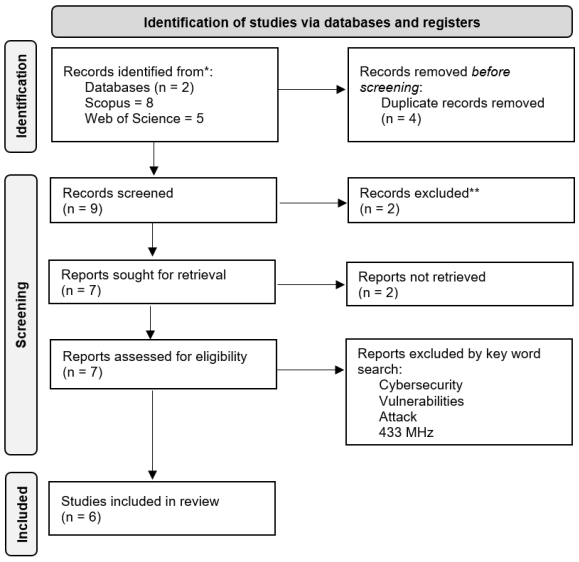

Figure 3. PRISMA Flowchart. *Number of records identified in each database. **Records excluded from the database based on the search criteria.

To ensure the selection of relevant articles, a structured search query was carried out using key terms combined with the Boolean operators "AND" and "OR": "cyber_securit", "vulnerabilit*", "attack*", "433_MHz*". After retrieving the set of articles from the Scopus and Web of Science databases, the results were merged and duplicates were removed using the Bibliometrix 4.1.3 package implemented in R 4.3.2 [R Core Team 2025]. As a result, a final set of six unique articles was obtained, which formed the basis for the qualitative analysis.

3.2. Common Vulnerabilities and Exposures (CVE®)

The CVE system, created by MITRE in 1999, is a global standard for identifying and naming known vulnerabilities in software and hardware, enabling interoperability between security tools and databases [MITRE Corporation 2025]. Complementary resources include the National Vulnerability Database (NVD), which enriches CVE entries with structured data such as CVSS scores and failure classifications [NIST 2025, FIRST 2025a]. To enhance risk prioritization, the Exploit Prediction Scoring System (EPSS) estimates the likelihood of exploitation using machine learning [FIRST 2025b], while the CISA's Known Exploited Vulnerabilities (KEV) catalog highlights vulnerabilities with confirmed active exploitation [CISA 2025].

The procedure for analyzing documented vulnerabilities in devices operating in the 433 MHz band was divided into three stages. First, relevant CVEs were identified through searches in the CVE.org and NIST NVD databases using the keyword "433 MHz". As examples, CVE-2023-31762, which describes a replay attack vulnerability in remote keyless entry systems, and CVE-2020-9550, which involves the transmission of sensitive data in plaintext, were among the most critical entries found.

Next, key attributes were extracted from each entry, including the CVE ID, attack vector, type of threat, type of vulnerability, affected layer, CVSS score, EPSS and KEV. Finally, an association was made between CVE, vulnerability type, and attack type, resulting in a structured table that served as the basis for the results analysis and the construction of experimental scenarios.

3.3. RF Cyber Range: Scenario

3.3.1. Tools: GNU Radio and RTL-SDR

The RTL-SDR is a low-cost and easily accessible software-defined radio (SDR) device, commonly used for monitoring, spectrum analysis, and wireless system security applications [RTL-SDR 2025, Hung and Vinh 2019]. In this work, the RTL-SDR was used as a tool for receiving, inspecting, and experimentally analyzing signals transmitted in the 433 MHz band, enabling the identification and analysis of vulnerabilities in radio frequency communication devices.

GNU Radio is an open-source platform used for the development of software-defined radio (SDR) systems, enabling the creation of real-time signal processing flowgraphs through modular blocks and an intuitive graphical interface [GNU Radio 2025]. In this work, GNU Radio was employed to build experimental communication scenarios in the 433 MHz band, allowing for the simulation, analysis, and execution of controlled attacks, such as jamming and replay, with the aim of identifying vulnerabilities in RF devices.

3.3.2. ASK-OOK Demodulation of Devices in 433 MHz

The reception of ASK-OOK modulated signals with GNU Radio begins with the conversion of these signals into digital data. This process is carried out by the RTL-SDR dongle or any other compatible device available on the market. The block diagram of the receiver is shown in Figure 4.

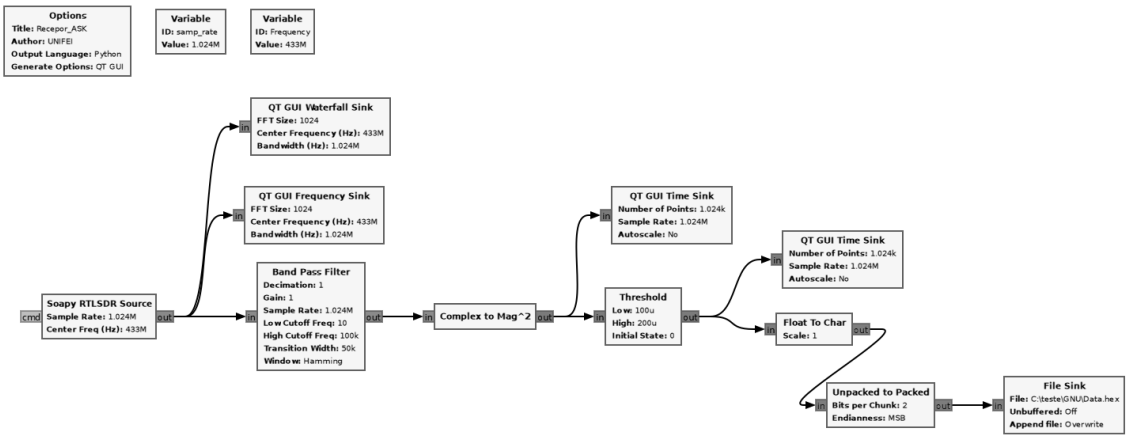

Figure 4. Block diagram for ASK-OOK demodulation in GNU Radio.

To analyze the captured spectra, the RTL-SDR output is connected to two blocks: one applies the Fourier transform to visualize the frequency spectrum and amplitude, and the other displays signal intensity over time (waterfall plot). For demodulation, a 100 kHz band-pass filter, typical of 433 MHz devices such as garage door openers and alarm systems, removes unwanted noise and interference prior to digital processing.

After filtering, the signal is converted into squared magnitude by the Complex to Mag² block and visualized in real time using the QT GUI Time Sink. A threshold detector identifies the bits ”0” and ”1” based on the amplitude, providing a digital output, in a process similar to that of analog demodulators built with discrete components. For the purpose of data analysis, the received bits were converted into bytes and then saved to a file. These functions were performed using the blocks “Float to Char”, “Unpacked to Packed”, and “File Sink”. Figure 5 below illustrates the program in operation.

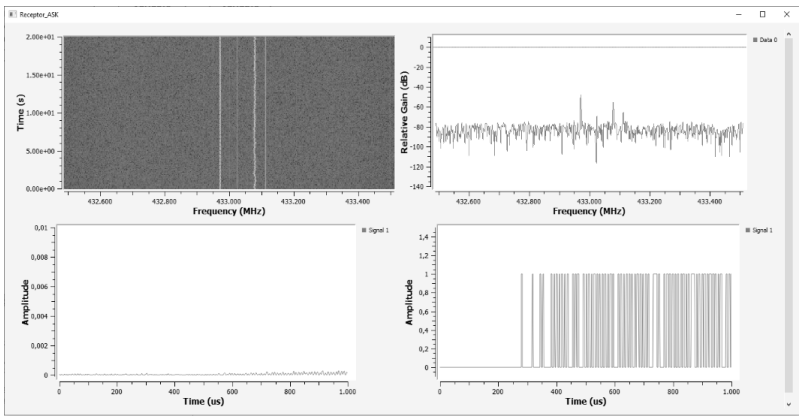

Figure 5. Graphical interface for visualizing data from the SDR device.

3.4. Denial-of-Service Attack

As shown, signal detection from remote controls, such as those used in alarms, vehicles, and gates, relies on the amplitude of the received signal. An attacker can disrupt this by generating a strong signal that saturates the receiver, disrupting normal operation and causing the output to remain fixed at a logical zero or one. This vulnerability was validated in two scenarios: a simulated jamming attack using GNU Radio (Figure 6), and a real-world experiment in which a signal generator blocked the reception of a remote control.

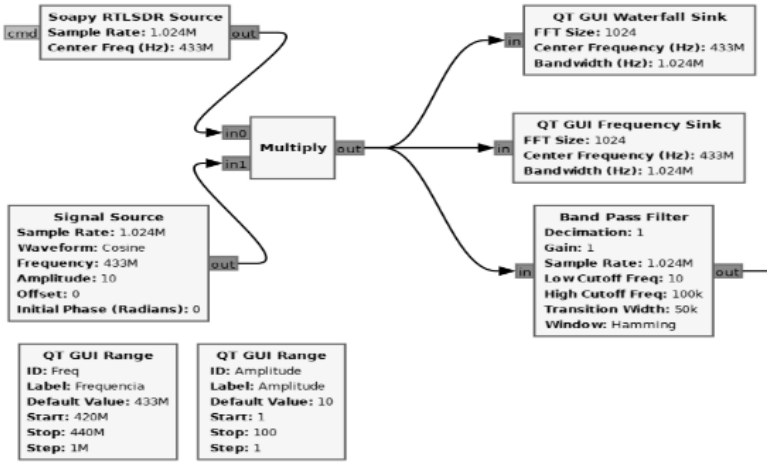

Figure 6. Block diagram for simulating denial-of-service attacks on ASK-OOK modulations in GNU Radio.

In the simulated environment, the insertion of a carrier signal, which, depending on its intensity, can lead the receiver circuit to saturation, is achieved by adding a sine wave signal generator block that is summed with the received RF signal before the filtering circuit and demodulation stage. For greater control over the effects of this attack, two adjustment sliders were added using QT GUI Range blocks to control the amplitude and frequency of the interfering signal. The result of this modification is shown in Figure 7.

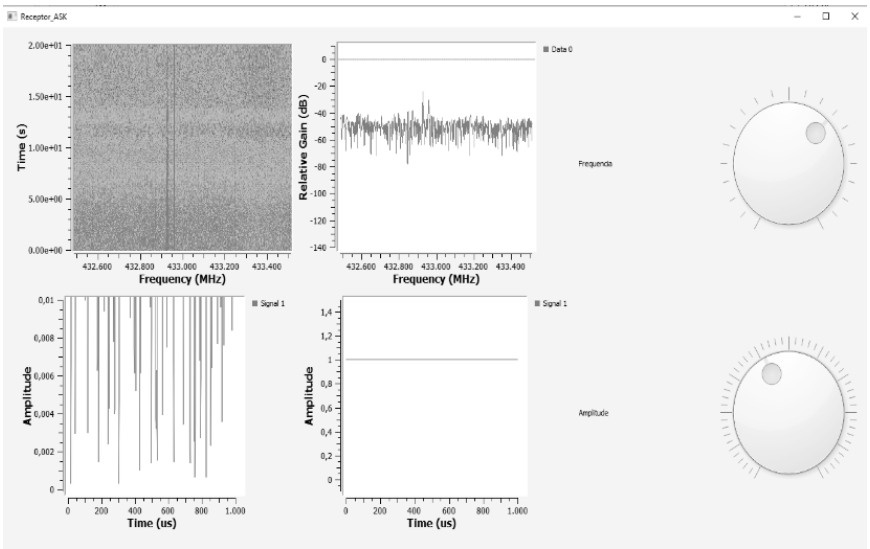

Figure 7. Graphical interface for visualizing the denial-of-service (DoS) attack.

It is possible to observe that, even without fully saturating the signal, as shown in the lower left graph, the signal level remained above the threshold level of the detector, resulting in a constant output bit of one.

4. Results and Discussion

4.1. Scientometric Analysis Results

The following presents the main results obtained from the scientometric analysis focused on cybersecurity in the 433 MHz band. The objective of this analysis was to identify trends, gaps, and patterns in the scientific literature on the topic, providing an overview of the main vulnerabilities, attack techniques, and mitigation strategies discussed in the literature. These results served as a basis for the construction of the scenarios used in the RF Cyber Range.

Figure 8 shows a modest yet growing trend in publications related to cybersecurity in the 433 MHz band. After isolated entries in 2011 and 2017, there has been a renewed interest starting in 2022, with 2024 standing out as the year with the highest number of publications (two articles). This growth may be associated with the popularization of IoT applications and the rising concern over vulnerabilities in low-cost wireless devices, such as sensors, alarm systems, and remote controls, which often operate in this frequency band.

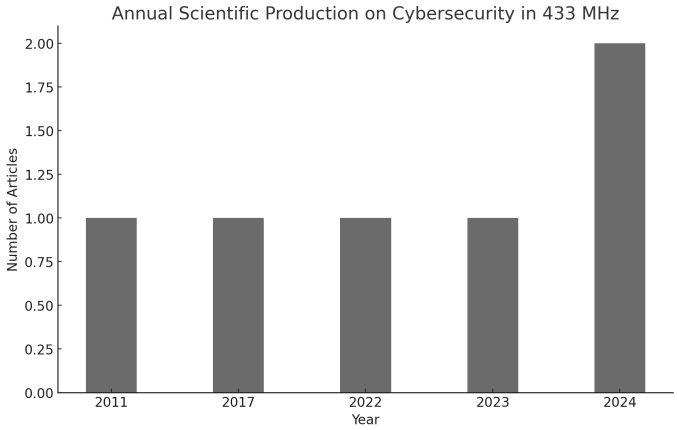

Figure 8. Annual scientific production.

Although the total number of studies is still limited, some articles already demonstrate significant impact in the field. Notable examples include the work by [Lee et al. 2017] with 19 citations, and [Muñoz et al. 2023] with 15 global citations, indicating recognition by the scientific community. Also worth highlighting are the studies by [Kasper et al. 2011, Allen et al. 2024], which contribute to the consolidation of the topic and demonstrate the growth potential of research in cybersecurity applied to systems operating in the 433 MHz band. The following is a literature review of the articles obtained in this analysis.

Allen et al. (2024) analyzed vulnerabilities in home security devices operating at 433 MHz, demonstrating jamming and replay attacks using low-cost tools such as HackRF One and RollJam. A total of 14 zero-day vulnerabilities were identified, five

of which were specific to this frequency band, with CVSS scores of up to 8.7, affecting brands such as AGSHome and Kerui. The study highlighted flaws even in certified devices like the Yale Conexis L1, and criticized the lack of response from manufacturers regarding the reported issues, underscoring the fragility of the ecosystem despite certifications such as TS 621.

Mykhaylova et al. (2024) demonstrated that the EV1527 protocol, widely used in 433 MHz remote controls, is vulnerable to replay attacks due to the use of fixed codes without encryption. Using tools such as HackRF One and Universal Radio Hacker, it was possible to capture and retransmit valid signals, compromising home automation systems. The study also evaluated the performance of receiving antennas and recommended, as a mitigation measure, the adoption of rolling code protocols, such as HCS301.

Muñoz et al. (2023) developed a test environment for cyberattacks on home IoT systems, demonstrating a replay attack against garage door remotes operating in the 433 MHz band. Using tools such as NESDR Smart, Arduino, and GNU Radio, they were able to open the door in under two seconds. The vulnerability was attributed to the lack of encryption, rolling code, and proximity-based authentication. The study suggests mitigation through the use of protocols in the 866 MHz band and complementary authentication via Bluetooth Low Energy (BLE).

Najath et al. (2022) presented a portable jammer based on Arduino for the 433 MHz band, capable of disrupting wireless communications at distances of up to 100 meters. The device uses modulated pulses to generate interference and demonstrated effective blocking in practical tests. The study warns of the legal risks associated with the use of jammers and suggests its future adaptation for other frequency bands, such as Wi-Fi and cellular networks.

Lee et al. (2017) proposed a wireless authentication tag operating at 433 MHz, designed to resist physical and side-channel attacks for use in critical applications. The tag employs the Keccak algorithm with query-based key updating, non-volatile flip-flops, and power backup to ensure integrity during failures. Using PPM (Pulse Position Modulation) for communication, it operates with low power consumption and high reliability, although it exposes the chip ID and key index, which allows for tracking. The solution stands out for combining cryptographic security with fault tolerance, making it suitable for mission-critical environments.

Kasper et al. (2011) demonstrated that active RFID devices and remote controls operating at 433 MHz are vulnerable to attacks such as eavesdropping, sleep deprivation, and man-in-the-middle (MITM), even when using simple equipment such as a USRP and a Yagi-Uda antenna. Communications were intercepted at distances of up to 500 meters, and devices were detected at up to 1000 meters. A battery exhaustion attack drained an RFID device in less than an hour. The authors warned of risks such as tracking, cloning, and malware injection, and recommended countermeasures such as encryption, distance-based authentication, and physical barriers.

4.2. Analysis of Vulnerabilities in the Literature on Cybersecurity in 433 MHz

The following analysis compiles information extracted from the articles obtained through the scientometric study, highlighting vulnerabilities, impacts, mitigation strategies, and types of attacks affecting devices that operate in the 433 MHz frequency band. These data

were organized into clear and structured tables, allowing for an objective understanding of the risks associated with this communication band.

Table 1 summarizes the vulnerabilities extracted from the six analyzed articles, revealing recurring flaws in devices operating in the 433 MHz band.

Table 1. Vulnerabilities identified in the literature for the 433 MHz band.

Article	Type of Vulnerability	Exploitation Effects	Suggested Mitigations
Allen *et al.* (2024)	Lack of authentication, fixed code, no jamming detection, lack of encryption	Compromise of alarms and locks; unauthorized access	Rolling code, jamming detection, OTA updates
Mykhaylova *et al.* (2024)	Fixed code, lack of encryption	Unauthorized access to control systems	Use of protocols with rolling code
Muñoz *et al.* (2023)	Fixed code, lack of encryption, lack of proximity authentication	Unauthorized opening of garage doors	Use of 866 MHz rolling code, BLE-based authentication
Najath *et al.* (2022)	Susceptibility to intentional interference (jamming)	Communication blocking between devices	Expand operating range, integrate Wi-Fi/cellular
Lee *et al.* (2017)	Exposure of chip ID and key index (traceability)	Tracking risk; authentication failure	Query-based updates, glitch detection
Kasper *et al.* (2011)	Exposure to passive eavesdropping, tracking, exhaustion attacks (sleep deprivation), MITM	Cloning, tracking, battery depletion	Encryption, distance-based authentication, physical barriers

Table 1 highlights key issues such as fixed codes, lack of encryption, and the absence of authentication, enabling unauthorized access, cloning, and tracking. Vulnerabilities to jamming and energy exhaustion were also observed, affecting system availability. Suggested mitigations include rolling codes, OTA updates, integration into Wi-Fi and cellular networks, and proximity-based authentication, emphasizing the need for more secure and modern solutions.

Table 2 summarizes the main types of attacks documented in studies on cybersecurity in the 433 MHz band. Jamming (DoS) and replay attacks appear most frequently, highlighting vulnerabilities in the physical and data link layers. The tools used include low-cost devices such as HackRF One, RollJam, Arduino, NESDR, and USRP, reinforcing the feasibility of low-cost, low-complexity attacks. More advanced threats were also observed, such as power glitch and man-in-the-middle (MITM) attacks. Vulnerable devices include remote controls without rolling codes, active RFID tags, and systems using the EV1527 protocol, revealing concrete security risks for both commercial and residential applications.

Table 2. Types of attacks in 433 MHz RF communication, based on the literature.

Article	Type of Attack	Tools Used	Affected Layer	Vulnerable Devices
Allen *et al.* (2024)	Jamming (DoS), Replay	HackRF One, RollJam, Yardstick One, Baofeng UV-5R	Physical, Link	AGSHome, Blitzwolf, Digoo, Kerui, WAFU
Mykhaylova *et al.* (2024)	Replay	HackRF One, Universal Radio Hacker, GQRX	Physical, Link	Devices with EV1527 protocol
Muñoz *et al.* (2023)	Replay	NESDR Smart, Arduino 433 MHz, GNU Radio	Physical	Remote controls without rolling code
Najath *et al.* (2022)	Jamming (DoS)	Arduino Nano, 433 MHz RF module, OLED	Physical	Devices without jamming protection
Lee *et al.* (2017)	Replay, Power Glitch	CMOS 130nm, Keccak, NVDFF	Physical, Application	N/A
Kasper *et al.* (2011)	Eavesdropping, Sleep Deprivation, Man-in-the-Middle (MITM)	USRP, Yagi-Uda, GNU Radio, GPS	Physical, Link	Active RFIDs ISO 18000-7

4.3. Analysis of CVEs Related to the 433 MHz Band

This section analyzes vulnerabilities documented in the CVE database that are associated with devices operating at the 433 MHz frequency. The information was organized into tables detailing the types of vulnerabilities, impact, attack types, and affected devices, providing insight into the real-world risks involving radio frequency-based systems.

Table 3 shows that most of the identified vulnerabilities are associated with CWE-294, which relates to replay attacks that compromise authentication and allow actions such as disarming alarms, unlocking locks, and unauthorized access to vehicles. This concentration reveals a common weakness in the protection of devices operating in the 433 MHz band: the absence of robust authentication mechanisms. Also noteworthy is CVE-2020-9550, associated with CWE-319, which involves the transmission of sensitive data in plaintext and received the highest score in the analysis (CVSS 9.8). Additionally, access control failures CWE-284 highlight risks to the integrity and availability of systems. The impact of the CVEs ranges from 4.6 to 9.8, with a predominance of high or critical ratings, indicating serious vulnerabilities in devices and security within the 433 MHz band.

Table 3. Classification of CVEs associated with vulnerabilities in 433 MHz.

CVE ID	Type of Vulnerability	Exploitation Effects	CVSS	EPSS (%)	KEV
CVE-2023-50128	CWE-294 – Authentication Bypass via Capture and Replay	Unauthorized disarming of the alarm system	5.3 (Medium)	0.0029%	No
CVE-2023-31763	CWE-294 – Authentication Bypass via Capture and Replay	Full access to the alarm system	7.5 (High)	0.0018%	No
CVE-2023-31761	CWE-294 – Authentication Bypass via Capture and Replay	Unauthorized disarming of the alarm system	7.5 (High)	0.0017%	No
CVE-2023-31762	CWE-294 – Authentication Bypass via Capture and Replay	Unauthorized disarming of the alarm system	7.5 (High)	0.0017%	No
CVE-2023-31759	CWE-294 – Authentication Bypass via Capture and Replay	Unauthorized disarming of the alarm system	7.5 (High)	0.0016%	No
CVE-2023-34553	CWE-294 – Authentication Bypass via Capture and Replay	Unauthorized unlocking of the lock	6.5 (Medium)	0.00069%	No
CVE-2022-45914	CWE-294 – Authentication Bypass via Capture and Replay	Unauthorized alteration of values displayed on electronic tags	6.5 (Medium)	0.29%	No
CVE-2022-38766	CWE-294 – Authentication Bypass via Capture and Replay	Unauthorized unlocking of the vehicle	8.1 (High)	0.79%	No
CVE-2020-9550	CWE-319 – Transmission of Sensitive Information in Cleartext	Unauthorized control of home automation system devices	9.8 (Critical)	—	No
CVE-2019-9659	CWE-294 – Authentication Bypass via Capture and Replay	Unauthorized disarming of the alarm system	9.1 (Critical)	—	No
CVE-2019-11561	CWE-284 – Improper Access Control	Disruption of proper operation of the alarm system	5.9 (Medium)	0.003%	No
CVE-2018-11401	CWE-284 – Improper Access Control	Disruption in communication between sensors and the alarm system's central unit	4.6 (Medium)	0.14%	No

Table 3 also presents risk metrics related to the likelihood of exploitation (EPSS) and the presence of vulnerabilities in official catalogs of actively exploited threats (KEV). The Exploit Prediction Scoring System (EPSS) values are predominantly low, ranging from 0.00069% to 0.79%, which suggests that, although technically exploitable, these vulnerabilities currently have a low probability of being exploited in the wild. Further-

more, none of the listed CVEs appear in the Known Exploited Vulnerabilities (KEV) catalog maintained by CISA, indicating that there are no official records of confirmed exploitation by threat actors according to U.S. cybersecurity authorities.

This gap stems from three factors: (i) most of these vulnerabilities occur in consumer-grade devices, which are rarely covered in institutional cybersecurity reports [Anthi et al. 2024]; (ii) attacks occur at the physical layer, making detection and tracking at scale difficult [Han et al. 2025]; and (iii) these devices lack automatic updates and incident response mechanisms, limiting the dissemination of evidence [ENISA 2020]. Therefore, these issues highlight the need for proactive mitigation and independent security assessments in unprotected RF bands such as 433 MHz.

Still referring to Table 3, although CVE-2020-9550 (CVSS 9.8) and CVE-2019-9659 (CVSS 9.1) are classified as critical according to the CVSS metric, they do not have an associated EPSS score. This is because the EPSS model, which uses machine learning to estimate the probability of exploitation in the wild, relies on empirical signals from public sources, such as exploit repositories, threat intelligence feeds, and malware scanners. Vulnerabilities affecting consumer-grade RF-based IoT devices, particularly those operating in local environments with limited exposure, often lack sufficient data to feed the EPSS model. As a result, even technically severe vulnerabilities may not receive an EPSS score when no large-scale exploitation or public indicators are available.

Table 4 presents the vulnerable devices listed in the analyzed CVEs, highlighting the predominance of replay attacks, all directly affecting the physical layer. Residential alarm systems, smart locks, and automotive devices make up the majority of targets, indicating that RF-based security solutions in the 433 MHz band are particularly susceptible to signal interception and replay. Cases of sniffing, spoofing, and denial-of-service (DoS) attacks were also identified, showing that, in addition to weak authentication, these devices lack protection mechanisms against interference and eavesdropping. The variety of affected brands and models demonstrates that the issue is widespread and not limited to a specific manufacturer.

Table 4. Types of attacks associated with CVEs in 433 MHz.

CVE ID	Type of Attack	Affected Layer	Vulnerable Devices
CVE-2023-50128	Replay Attack	Physical	Hazard alarm system v1.0
CVE-2023-31763	Replay Attack	Physical	AGShome Smart Alarm system v1.0
CVE-2023-31761	Replay Attack	Physical	RF devices with open communication
CVE-2023-31762	Replay Attack	Physical	Digoo DG-HAMB home security system v1.0
CVE-2023-31759	Replay Attack	Physical	Kerui W18 alarm system v1.0
CVE-2023-34553	Replay Attack	Physical	WAFU Keyless Smart Lock v1.0
CVE-2022-45914	Replay Attack	Physical	ESL electronic tags using RF transceiver OV80e934802 on board ETAG-2130-V4.3 20190629
CVE-2022-38766	Replay Attack	Physical	Keyless entry system of Renault ZOE 2021
CVE-2020-9550	Sniffing and Spoofing	Physical	Rubetek SmartHome devices 2020
CVE-2019-9659	Replay Attack	Physical	Chuango alarm system and similar products, such as Eminent EM8617 OV2 Wifi Alarm System
CVE-2019-11561	Denial of Service (DoS)	Physical	433 MHz intrusion alarm product line from Chuango and similar products, such as Eminent EM8617 OV2 Wifi Alarm System
CVE-2018-11401	Jamming (DoS)	Physical	SimpliSafe Original alarm system

4.4. Scenario Results

4.4.1. RF Cyber Range (Simulated)

The file generated by the program allows the identification of data transmitted by a real transmitter operating at 433 MHz. The confirmation and identification of the encoding scheme used depend on the implementation of additional elements, which are beyond the scope of this work. Under normal conditions, without any attack, what is expected is a sequence of zero-value bytes for most of the time, and a set of values appearing when the transmitter is activated nearby. Figure 9 illustrates this situation.

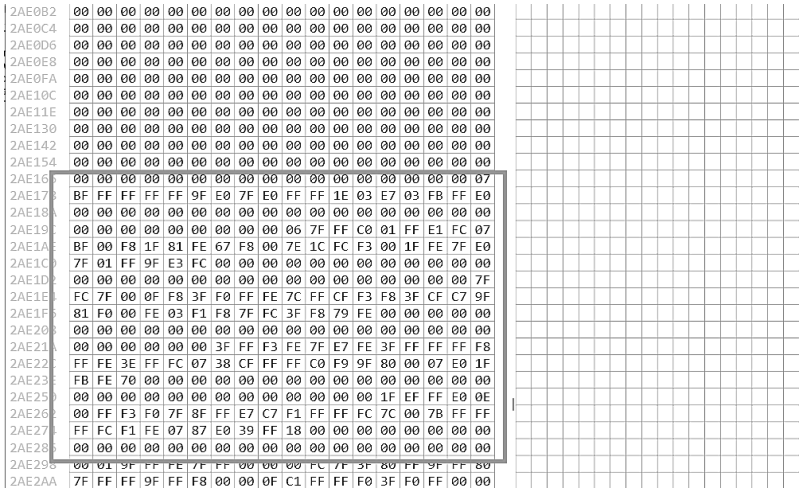

Figure 9. Sequence of bytes received.

Repeating the experiment, this time with an interfering signal, as expected, the receiver recorded a response consisting of a sequence of values corresponding to bit one (see Figure 10).

Figure 10. Receiver under jammer attack.

Although inevitable, this type of attack can be easily detected, as long consecutive sequences of ones do not correspond to the expected behavior of a normally functioning system of this type.

4.4.2. RF Cyber Range (Laboratory)

To study and analyze the impact of an intentional interference signal (jammer) on circuits operating in the 433 MHz band, an experiment was conducted in a controlled laboratory environment. The following equipment was used: one MG3710A Vector Signal Generator (Anritsu); one Directional Antenna (Aaronia AG); one notebook running GNU Radio

Companion v. 3.10.12.0; one RTL-SDR receiver; and one remote control device. Figure 11 shows the experimental setup used.

Figure 11. Laboratory experimental setup.

Initially, the experiment was conducted in the absence of the interference signal, confirming the proper functioning of the receiver composed of GNU Radio and RTL-SDR, with the correct detection of the signals emitted by the remote control. In the next stage, the vector signal generator was connected to the directional antenna and configured to emit interference signals (jammer) with power levels ranging from -60 dBm to 0 dBm. It was observed that for power levels above -40 dBm, the threshold detection block of the ASK-OOK demodulator entered saturation. Under this condition, the demodulator circuit became inoperative, and the overall system behavior was similar to that observed in equivalent tests using a signal generator implemented with blocks in GNU Radio.

To expand the scope of the experimental analysis, future studies are encouraged to incorporate thresholds for Bit Error Rate (BER) and Signal-to-Noise Ratio (SNR) under varying levels of interference. These metrics will enable a more accurate quantitative assessment of system robustness and will aid in characterizing signal integrity degradation in realistic interference scenarios.

4.5. Ethical, Legal, and Strategic Considerations for Using SDR

SDRs are widely used for various purposes by amateur radio operators and hobbyists due to their flexibility and accessibility. However, even in unlicensed frequency bands such as 433 MHz, their use is subject to regulations established by agencies such as ANATEL, the FCC, and the ITU-R. Disregarding these guidelines may cause interference with legitimate systems and result in unauthorized or unlawful spectrum usage.

Although the tests in this study were conducted in a controlled environment, in compliance with legal and ethical standards, it is essential to consider the broader implications of these experiments. The identified vulnerabilities, particularly those related to the lack of encryption and authentication, reveal real risks in 433 MHz RF devices. However, the absence of CVEs related to this frequency band in catalogs such as KEV, along with low EPSS scores, indicates that these threats remain overlooked and lack formal channels for patching or updates.

It is also important to note that certain SDR-based devices, such as the HackRF One, while legally sold and used for passive reception and academic experimentation, may violate national regulations if employed for unauthorized transmission. Moreover, devices explicitly designed for signal jamming, such as FlipFlop-style jammers, are prohibited under Brazilian law, as they intentionally cause harmful interference. According to the Brazilian Telecommunications Law (Law No. 9.472/1997, Art. 183) and ANATEL Resolution No. 680/2017, unauthorized transmission or interference in radio communications is considered an illicit act. Therefore, researchers and practitioners must ensure full compliance with local regulations when using SDR equipment for security testing [Brazil 1997, Anatel 2017].

In this context, this study acknowledges that experiments involving SDRs must be conducted with ethical responsibility, and that manufacturers should implement security mechanisms, such as strong authentication and encryption, even in low-cost devices. It is also recommended that regulatory agencies establish baseline security requirements for the certification of RF devices. Furthermore, the findings presented here should be shared with standardization bodies and incident response centers, such as the Brazilian Computer Emergency Response Team [CERT.br 2025], in order to promote concrete mitigation actions and strengthen cybersecurity in wireless communication devices.

5. Conclusion

This study investigated vulnerabilities in devices operating in the 433 MHz band, highlighting the lack of authentication and encryption as a critical factor enabling attacks such as jamming and replay. The methodology combined scientometric analysis, CVE analysis, and practical testing using GNU Radio and RTL-SDR, validating the feasibility of such attacks using accessible tools.

The results reveal recurring flaws at the physical layer, with direct impact on the availability and integrity of IoT and automation systems. These findings underscore the need for the adoption of security measures, such as dynamic protocols and proximity-based authentication, even in low-cost devices. Moreover, despite the effectiveness of the tests, the study was limited to ASK-OOK devices and did not incorporate quantitative metrics such as BER and SNR.

For future research, it is recommended to include spoofing attacks, real-time detection techniques, and the development of open repositories for educational and research purposes. Therefore, in the face of increased connectivity, ensuring security in RF systems is essential to mitigate growing risks and to promote safer practices in radio frequency communications.

6. Acknowledgments

The authors would like to thank the Federal University of Itajubá (UNIFEI), CNPq, CAPES, Clavis Information Security (FINEP/Plat-Ciber) for its financial support in CyberOT Project, Cyber Intelligence Laboratory (LInC), and the u.AI, FronTIERS HackLab, LabTel and LAIoT laboratories for their technical support.

References

Abdul-Ghani, H. A. and Konstantas, D. (2019). A comprehensive study of security and privacy guidelines, threats, and countermeasures: An iot perspective. *Journal of Sensor and Actuator Networks*, 8(2):22.

Allen, A., Mylonas, A., Vidalis, S., and Gritzalis, D. (2024). Smart homes under siege: Assessing the robustness of physical security against wireless network attacks. *Computers & Security*, 139:103687.

Anatel (2017). National telecommunications agency. Technical Report 680, Anatel. Resolution No. 680 of June 27, 2017: Regulation on Restricted Radiation Radiocommunication Equipment.

Anatel (2025). National telecommunications agency. https://www.gov.br/anatel.

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.

Brazil (1997). Law no. 9.472 of july 16, 1997: General telecommunications law.

CERT.br (2025). Computer emergency response team brazil. https://www.cert.br/. Brazilian National CSIRT of Last Resort.

CISA (2025). Cybersecurity and infrastructure security agency. https://www.cisa.gov/known-exploited-vulnerabilities. Known Exploited Vulnerabilities (KEV) Catalog.

ENISA (2020). European union agency for cybersecurity. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things. Guidelines for Securing the Internet of Things (IoT),.

FIRST (2025a). Common vulnerability scoring system v3.1: Specification document. https://www.first.org/cvss/.

FIRST (2025b). Exploit prediction scoring system (epss). https://www.first.org/epss/.

GNU Radio (2025). Gnu radio. https://www.gnuradio.org/.

Han, M., Yang, H., Li, W., Xu, W., Cheng, X., Mohapatra, P., and Hu, P. (2025). Rf sensing security and malicious exploitation: A comprehensive survey. *arXiv preprint*, arXiv:2504.10969.

Hung, P. D. and Vinh, B. T. (2019). Vulnerabilities in iot devices with software-defined radio. In *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, pages 1–5.

ISI Web of Science (2025). Isi web of science. https://www.webofscience.com.

ITU (2010). International telecommunication union. Report SM.2180. Impact of Industrial, Scientific and Medical (ISM) Equipment on Radiocommunication Services.

ITU (2025). International telecommunication union. https://www.itu.int/en/ITU-R/Pages/default.aspx. ITU Radiocommunication Sector (ITU-R).

Kasper, T., Oswald, D., and Paar, C. (2011). Wireless security threats: Eavesdropping and detecting of active rfids and remote controls in the wild. In *Proceedings of the 19th*

International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pages 1–6. IEEE.

Kumbhar, A. (2017). Overview of ism bands and software-defined radio experimentation. *Wireless Personal Communications*, 97:3743–3756.

Lau, F., Rubin, S. H., Smith, M. H., and Trajkovic, L. (2000). Distributed denial of service attacks. In *Proceedings of the SMC 2000 Conference Proceedings, 2000 IEEE International Conference on Systems, Man and Cybernetics: 'Cybernetics Evolving to Systems, Humans, Organizations, and Their Complex Interactions'*, volume 3, pages 2275–2280, Nashville, TN, USA. IEEE.

Lee, H.-M., Juvekar, C. S., Kwong, J., and Chandrakasan, A. P. (2017). A nonvolatile flip-flop-enabled cryptographic wireless authentication tag with per-query key update and power-glitch attack countermeasures. *IEEE Journal of Solid-State Circuits*, 52(1):272–283.

MITRE Corporation (2025). Common vulnerabilities and exposures (cve®). https://cve.mitre.org.

Muñoz, A., Fernández-Gago, C., and López-Villa, R. (2023). A test environment for wireless hacking in domestic iot scenarios. *Mobile Networks and Applications*, 28:1255–1264.

Mykhaylova, O., Stefankiv, A., Nakonechny, T., Fedynyshyn, T., and Sokolov, V. (2024). Resistance to replay attacks of remote control protocols using the 433 mhz radio channel. In *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2024)*, volume 3654, Kyiv, Ukraine. CEUR Workshop Proceedings.

Najath, M. N. M., Herath, H. M. D. S., and Rajapakse, A. (2022). Design and testing of an arduino-based network jammer device. In *2022 7th International Conference on Information Technology Research (ICITR)*, pages 1–6.

NIST (2025). National institute of standards and technology. https://nvd.nist.gov/vuln. National Vulnerability Database (NVD).

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., et al. (2021). The prisma 2020 statement: An updated guideline for reporting systematic reviews. *Systematic Reviews*, 10:89.

R Core Team (2025). *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria.

Ribeiro, J. A. J. (2008). *Electromagnetic Wave Propagation: Principles and Applications*. Érica Publishing, 2nd edition.

RTL-SDR (2025). Rtl-sdr (software defined radio). https://www.rtl-sdr.com/.

Scopus (2025). Scopus. https://www.scopus.com.

Zhu, J. and Liu, W. (2020). A tale of two databases: The use of web of science and scopus in academic papers. *Scientometrics*, 123:321–335.