Article

Not peer-reviewed version

Practical Realization of Reactive Jamming Attack on LoRaWAN Network

Josip Sabic *, Toni Perković *, Dinko Begušić, Petar Šolić

Posted Date: 5 March 2025

doi: 10.20944/preprints202503.0355.v1

Keywords: LoRaWAN; reactive jamming; Internet of Things (IoT); security; countermeasures

Article

Practical Realization of Reactive Jamming Attack on LoRaWAN Network

Josip Šabić [1,†], Toni Perković [1,2,*,†], Dinko Begušić [1] and Petar Šolić [1]

[1] Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture in Split, University of Split, Croatia
[2] Corresponding author email: toperkov@fesb.com
* Correspondence: toperkov@fesb.com
† These authors contributed equally to this work.

Abstract: LoRaWAN networks are increasingly recognized for their vulnerability to various jamming attacks, which can significantly disrupt communication between end nodes and gateways. This paper explores the feasibility of executing reactive jammers upon detecting packet transmission using commercially available equipment based on Software-Defined Radios (SDRs). The proposed approach demonstrates how attackers can exploit packet detection to initiate targeted interference, effectively compromising message integrity. Two distinct experimental setups, one using separate SDRs for reception and transmission, and another leveraging a single SDR for both functions, were used to evaluate attack efficiency, reaction times, and packet loss ratios. Our experiments demonstrate that both scenarios effectively jam LoRaWAN packets across a range of spreading factors and payload sizes. This finding underscores a pressing need for enhanced security measures to maintain reliability and counter sophisticated attacks.

Keywords: LoRaWAN; reactive jamming; Internet of Things (IoT); security; countermeasures

1. Introduction

The Internet of Things (IoT) has revolutionized modern information systems by enabling seamless, large-scale connectivity among diverse devices. This ecosystem spans sensors, actuators, and mobile devices that communicate via standard network protocols. While short-range applications frequently employ GHz-based technologies (WiFi, Bluetooth, ZigBee), long-range communications require more energy-efficient solutions, namely Low-Power Wide-Area (LPWA) networks operating in the MHz band. [1–5].

LPWA networks are fundamental to the development of smart ecosystems, including urban infrastructure, agriculture, and industrial monitoring. Their capabilities - extended coverage (up to 15 km outdoors), minimal energy consumption, and low data rates - make them ideal for applications such as environmental monitoring, smart lighting, waste management, and precision agriculture [6,7]. LoRa technology, in particular, stands out for its ability to support long-range communication while ensuring extended battery life for IoT devices, facilitating deployments in remote or inaccessible locations [8,9].

Operating within unlicensed industrial, scientific and medical (ISM) frequency bands, LoRa, SigFox, and NB-IoT networks exhibit distinct characteristics in terms of communication modes, data rates, and cost of deployment. LoRa employs Chirp Spread Spectrum (CSS) modulation, while LoRaWAN utilizes this radio technology alongside a specific MAC layer to manage network communications. Frequency plans, channel assignments, spreading factors, and payload capacities vary regionally, with the European sub-1 GHz band encompassing 863 to 879 MHz and 433 MHz [10].

However, LoRaWAN's architecture also presents significant security challenges. The absence of centralized coordination for medium access control (MAC) increases susceptibility to network congestion and malicious interference. In particular, energy depletion attacks (EDA) threaten battery-powered devices [11], while frame collisions, duty cycle limitations (typically 1% under ETSI regulations), and

 doi:10.20944/preprints202503.0355.v1

uncoordinated transmissions amplify the vulnerability of the network [12–15]. These limitations become more pronounced as network density increases, with future deployments anticipated to involve thousands of devices operating within a single gateway's range.

One critical threat to LoRaWAN networks is jamming, where malicious actors transmit disruptive signals to interfere with legitimate communication. This type of attack can undermine essential IoT applications, including alarm systems, fire detection, and environmental monitoring [16,17]. Jamming can target specific channels or spreading factors, with reactive jamming being particularly effective. In this method, attackers identify active transmissions and promptly emit interfering signals, disrupting packet delivery while minimizing their transmission footprint to avoid detection [18].

This study explores the feasibility of executing reactive jamming attacks on LoRaWAN networks using commercially available software-defined radios - SDRs (under 1000 EUR). The proposed approach demonstrates how attackers can exploit packet detection to initiate targeted interference, effectively compromising message integrity. Through two distinct experimental setups—one using separate SDRs for reception and transmission, and another leveraging a single SDR for both functions—this paper evaluates attack efficiency, reaction times, and packet loss ratios. The results highlight the significant vulnerability of LoRaWAN to low-cost jamming strategies while discussing potential countermeasures to enhance network resilience against such threats [19–21].

2. Related Work - Jamming Attacks on LoRaWAN

2.1. LoRaWAN Vulnerability to Jamming

Due to LoRaWAN's reliance on the ALOHA protocol, which lacks collision-avoidance features, it remains highly susceptible to jamming attacks that disrupt communication between devices and gateways [22,23]. Selective jamming involves targeting specific packets or channels, while reactive jamming adapts its strategy based on the network response to interference, complicating detection and mitigation efforts [21,24].

Moreover, LoRaWAN-specific jamming techniques exploit the unique characteristics of LoRa's chirp spread spectrum modulation. Studies have shown that synchronized jamming can effectively disrupt LoRa communications by overwhelming the gateway with noise, leading to a dramatic decrease in network throughput [24,25]. The inherent design of LoRaWAN, which prioritizes long-range communication over robustness against interference, further exacerbates its vulnerability to such attacks [23,26].

2.2. Effectiveness of Different Jamming Methodologies

The effectiveness of various jamming methodologies has been a focal point in recent research. Previous studies report a 56% throughput drop when LoRaWAN experiences continuous jamming [22,27]. Meanwhile, sweep jamming, a dynamic frequency-varying technique, has been proven especially potent against frequency-hopping systems, presenting an additional threat to LoRaWAN [26,28].

LoRa-specific jamming techniques, such as those utilizing the unique properties of chirp signals, have also been explored. These methods can exploit the physical layer vulnerabilities of LoRaWAN, effectively disrupting communications without the need for sophisticated equipment [24,26]. The combination of these jamming strategies highlights the urgent need for enhanced security measures within LoRaWAN networks to mitigate the risks posed by such attacks [23,29].

2.3. Real-Time Reactive Jamming on All LoRaWAN Channels

The implementation of real-time reactive jamming on all LoRaWAN channels presents a complex challenge that requires a nuanced understanding of both the jamming mechanisms and the underlying network architecture. A real-time reactive jammer can dynamically adjust its jamming strategy based on the detected activity within the network, maximizing its impact while minimizing the likelihood of detection [30,31].

 doi:10.20944/preprints202503.0355.v1

The technical details of the implementation reveal that SDR technology plays a crucial role in the development of effective jammers. SDR-based jammers can be programmed to monitor multiple channels simultaneously and adapt their jamming signals in real time, providing a significant advantage over traditional hardware-based jammers [32,33]. Low-cost hardware-based jammers, such as those utilizing Arduino platforms, have also been successfully deployed, demonstrating that effective jamming does not necessarily require expensive equipment [30,34].

However, optimization of jammer strategies is not without limitations and challenges. Processing latency can hinder the responsiveness of jammers, particularly in fast-paced environments where quick adaptations are necessary [31,35]. Furthermore, detection avoidance remains a critical concern, as jammer deployment must be carefully managed to evade countermeasures employed by network operators [24,31].

2.4. Feasibility of Real-Time Multichannel Reactive Jamming

The feasibility of implementing multichannel reactive jamming in real time is based on several key requirements. First, monitoring of the wideband spectrum is essential to identify active channels and adapt jamming strategies accordingly [29,32]. This capability allows jammers to target specific frequencies that are currently in use, thereby increasing the effectiveness of their interference.

Parallel processing of multiple signals is another critical requirement for successful multichannel jamming. Using advanced processing techniques, jammers can simultaneously disrupt multiple channels, complicating the network's ability to maintain communication [24,26]. Furthermore, adaptive jamming techniques that can bypass the frequency hopping mechanisms employed by LoRaWAN are vital to ensure sustained disruption [28,36].

Table 1. Comparison of Jamming Methods in LoRaWAN Studies

Study	Method Used	Multi-channel	All Spreading Factors	Low cost (< 1000 €)	Effective in all SF-Freq combinations	Hardware
Dossa et al. [37]	SDR-based minimal exposure jamming	✗	✗	✗	✗	USRP-2920
Perković et al. [31,35]	Low-cost Arduino jammer	✗	✗	✓	✗	LoRa module (SX1276)
Šabić et al. [38]	SDR-based reactive jamming	✓	✓	✓	✗	HackRF ONE
This paper Scenario I	SDR-based reactive jamming	✓	✓	✓	✗ / ✓	HackRF ONE
This paper Scenario II	SDR-based reactive jamming	✓	✓	✓	✓	BladeRF

Demonstrated multichannel jamming architectures have shown promising results in various studies. For example, Šabić et al. [38] utilized SDR-based reactive jamming to effectively target multiple channels, while Perković et al. implemented a low-cost Arduino jammer that successfully disrupted single channel communications [30,31]. Dossa et al. also explored SDR-based minimal exposure jamming, highlighting the potential for sophisticated jamming strategies that minimize the risk of detection [37].

3. LoRa/LoRaWAN Message Transmission

This section provides an overview of how LoRa transmits messages, including key concepts such as Chirp Spread Spectrum (CSS) modulation, spreading factors, bandwidth, and frequency channels. In addition, it elaborates on the LoRaWAN network protocol, which is built on LoRa technology [10].

 doi:10.20944/preprints202503.0355.v1

3.1. Chirp Spread Spectrum (CSS) Modulation

LoRa relies on Chirp Spread Spectrum (CSS) modulation, spreading the signal across a broad bandwidth to bolster interference resilience—an attribute well-suited to long-range IoT deployments [39].

3.2. Carrier Frequency (CF)

LoRa operates in several frequency bands, with the most widely utilized frequencies falling within the sub-GHz range, specifically around 868 MHz in Europe and 915 MHz in North America. The selection of carrier frequency significantly affects both the transmission range and the penetration capabilities of the signal, where lower frequencies offer superior coverage, but at the cost of reduced data rates [39].

3.3. Coding Rate (CR)

The Coding Rate (CR) determines the proportion of redundancy bits included for error correction purposes. By adjusting the coding rate, a trade-off can be achieved between data rate and communication reliability: Higher coding rates improve resistance to noise and interference, but result in lower effective data throughput [39].

3.4. Spreading Factor (SF)

The Spreading Factor (SF) in LoRa modulation directly affects both data rate and interference resilience—higher SFs enhance reliability at the cost of slower throughput [40].

3.5. Bandwidth (BW)

The bandwidth (BW) configuration in LoRa directly affects both the spectral efficiency and the data transmission rate. A narrower bandwidth offers increased sensitivity and extended range, whereas a broader bandwidth supports higher data rates at the expense of coverage [40].

4. LoRaWAN

4.1. LoRaWAN Network Architecture

The LoRaWAN network architecture consists of end devices, gateways, and a network server that enables communication between devices and applications. The end devices equipped with LoRa transceivers transmit data to gateways, which then send it to the network server for processing before transmitting it to application servers [41]. LoRaWAN employs a star topology (Figure 1), comprising LoRa end devices, one or more gateways, and a centralized network server.

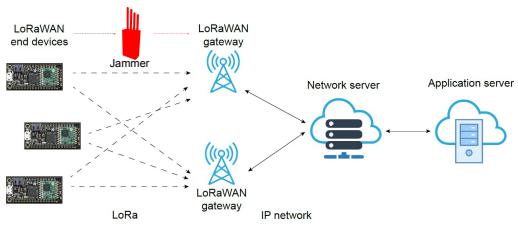

Figure 1. LoRaWAN (Long Range Wide Area Network) architecture.

4.2. End Devices

LoRaWAN end devices function as sensors or actuators that collect data from the environment or perform specific actions [41]. These devices are optimized for low power consumption, allowing them to operate for extended periods on battery power. LoRaWAN end devices are categorized into three classes: Class A, Class B, and Class C [42]. Class A devices transmit data only when necessary, ensuring energy efficiency. Class B devices are synchronized with periodic time slots to enable scheduled communications. Class C devices maintain continuous reception readiness for immediate downlink communication.

 doi:10.20944/preprints202503.0355.v1

4.3. LoRaWAN Packet Structure

A LoRaWAN packet consists of multiple fields, including the physical payload, MAC commands, and metadata for routing and error detection, as shown in Figure 2. The structured packet format ensures reliable and efficient communication between the end devices and the network infrastructure [41].

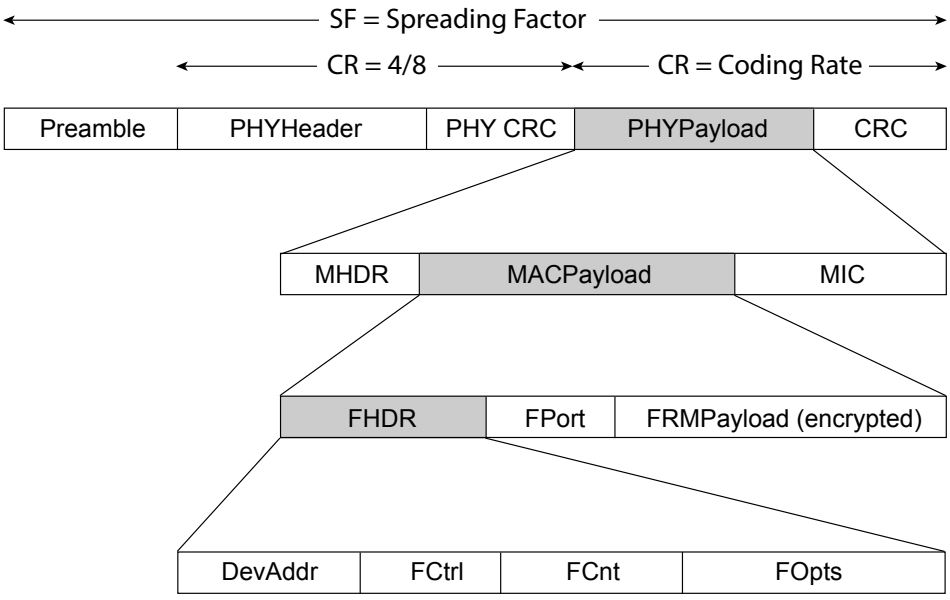

Figure 2. Structure of LoRaWAN (Long Range Wide Area Network) packet.

4.4. Threat Model

In this study, an active adversary model is considered in the context of LoRaWAN communication between the end nodes and the gateways. The attack scenario involves an adversary positioned between an end device and a gateway, monitoring the initiation of a LoRa transmission. Once the adversary detects the transmission, it determines key parameters such as frequency, spreading factor, and bandwidth. The attacker then transmits a high-power signal on the same channel and spread factor to prevent the legitimate message from reaching the gateway. If the jamming transmission successfully overlaps the original packet before it is complete, the attack effectively disrupts the communication.

5. Materials and Methods

This section details the experimental setup and methodology used to implement and evaluate the reactive jamming attack on LoRaWAN networks.

5.1. Hardware and Software Tools Used

- **Hardware**

  Our host computer featured a 12th Gen Intel® Core™ i7-1255U processor (10 cores, 12 threads, 1.7 GHz base, up to 4.7 GHz) and 8 GB of RAM, providing sufficient resources for processing and analyzing incoming radio signals.

  To support the experimental objectives, we employed SDRs, which are versatile communication systems where traditional hardware components, such as mixers, filters, and modulators, are implemented through software, allowing for greater flexibility and adaptability across various communication protocols and frequencies. The setup utilized two notable SDRs: the BladeRF and the HackRF One. Although not as expensive as high-end SDRs, these devices provided sufficient performance for experimental jamming studies.

  The BladeRF operates over a frequency range of 300 MHz to 3.8 GHz, offering up to 28 MHz of instantaneous bandwidth with software-selectable filter options ranging from 1.5 MHz to 28 MHz. It supports arbitrary sample rates of up to 40 MSPS with 12-bit IQ samples. The device

 doi:10.20944/preprints202503.0355.v1

is fully bus-powered over USB 3.0, ensuring high-speed data transfer, and includes an external power option via a 5V DC barrel jack.
The HackRF One covers frequencies from 1 MHz to 6 GHz and supports a maximum sample rate of 20 million samples per second with 8-bit quadrature sampling, enabling versatile transmission and reception capabilities. Together, the host computer and these SDRs provided a robust platform to analyze and manipulate radio signals across a broad spectrum, facilitating advanced wireless communication research and development. A limitation of the HackRF One is that it does not support full-duplex operation, which increases reaction time in certain setups.
For the LoRaWAN network components, we used the LILYGO TTGO T-Beam V1.0 as the end node device. This ESP32-based board features integrated LoRa (868/915MHz) and GPS capabilities, along with Wi-Fi and Bluetooth connectivity. As the gateway, we employed the Laird Sentrius RG1xx, an 8-channel LoRaWAN gateway supporting dual-band Wi-Fi and Ethernet connectivity, compatible with various LoRaWAN network servers.

- **Software**
The software implementation of the system was developed using GNU Radio, a powerful open-source software toolkit for building software-defined radios. GNU Radio enabled the modular design of the signal processing flowgraph, allowing seamless integration of various blocks for real-time detection and analysis of LoRaWAN signals. GNU Radio was chosen for its open source flexibility, allowing real-time signal processing without requiring expensive proprietary tools. Additionally, it offers extensive libraries and preexisting modulation/demodulation blocks for LoRa, simplifying implementation. It also provides seamless SDR integration with direct support for BladeRF and HackRF One devices.
A critical component of the setup was the ChirpDetector block, sourced from the gr-LibreLoRa library [1]. This block was instrumental in identifying LoRa chirps using their unique modulation characteristics, facilitating the extraction of parameters such as spread factor, bandwidth, and normalized frequency. The combination of GNU Radio's flexibility and the specialized capabilities of the ChirpDetector block ensured efficient and accurate signal processing.

5.2. Description of Experimental Setup

The experiments were carried out using two distinct scenarios to evaluate how different hardware configurations affect the efficiency of reactive jamming attacks on LoRaWAN networks.

- **Scenario 1: BladeRF as receiver, HackRF One as transmitter:**
Scenario I employs three devices—a BladeRF receiver, a HackRF One transmitter, and a host PC as illustrated in Figure 3 and shown in Figure 4. The BladeRF monitors the full EU LoRaWAN spectrum and forwards captured signals to the PC for processing to extract key parameters such as the SF, frequency, and BW. Based on the analysis, the HackRF One is used to transmit pre-recorded jamming packets on the detected frequency and SF, effectively interfering with legitimate LoRaWAN communication. This scenario mimics practical attack scenarios with affordable SDRs. We anticipated that this would be a cost-effective setup, offer flexible deployment, allow better control over hardware placement and synchronization testing, and allow decoupling of function for more precise monitoring of the jamming reaction time. However, we anticipated potential disadvantages, including increased latency due to communication between separate SDRs and synchronization challenges with hardware-dependent timing variations.

[1] https://gitlab.com/jpsimas/librelora

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 March 2025 doi:10.20944/preprints202503.0355.v1

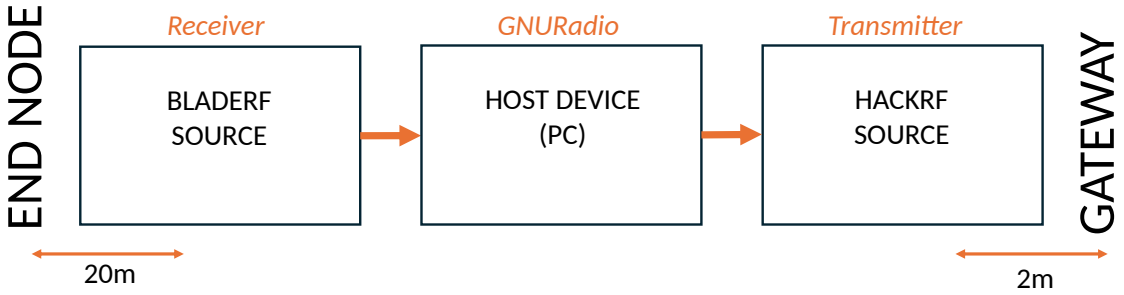

Figure 3. Scenario I block diagram setup.

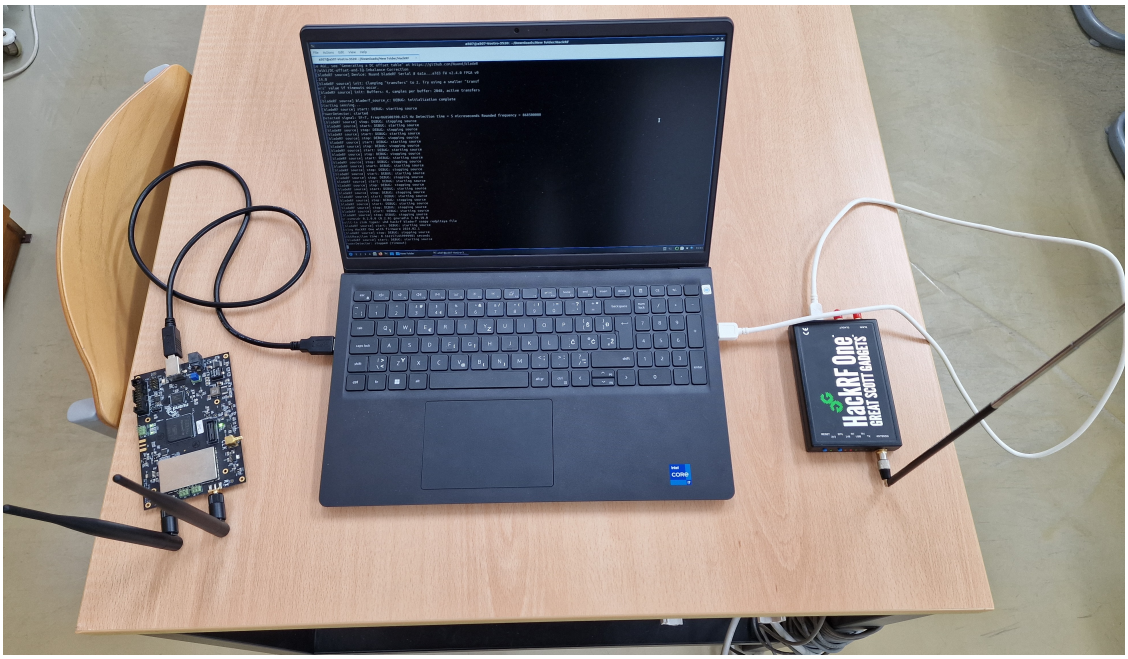

Figure 4. Scenario I setup.

- **Scenario 2: BladeRF as both receiver and transmitter:**
  In this scenario, only two devices are used: BladeRF and a host device (PC), as illustrated in Figure 5 and shown in Figure 6. The BladeRF SDR operates as both a receiver and a transmitter, monitoring all channels in the EU LoReWAN spectrum. The captured signals are processed on the host device, where relevant parameters are extracted. Once a target signal is detected, the BladeRF itself transmits the corresponding jamming packets on the detected frequency and SF, eliminating the need for a separate transmitter. This setup ensures a streamlined approach to signal acquisition and jamming within a single device. This scenario was designed to test the hypothesis that a single-device setup could lead to a faster jamming response. We anticipated that the advantages would include lower reaction time by eliminating the need for inter-device communication, improved synchronization by having both reception and transmission within the same SDR, and more efficient jamming due to reduced hardware switching time. However, we also anticipated disadvantages, including a higher processing load on the BladeRF, potentially introducing processing bottlenecks, limited flexibility for experimental variations requiring separate spatial positioning of the receiver and transmitter, and potential RF performance issues due to full-duplex operation in a single SDR.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 March 2025 doi:10.20944/preprints202503.0355.v1

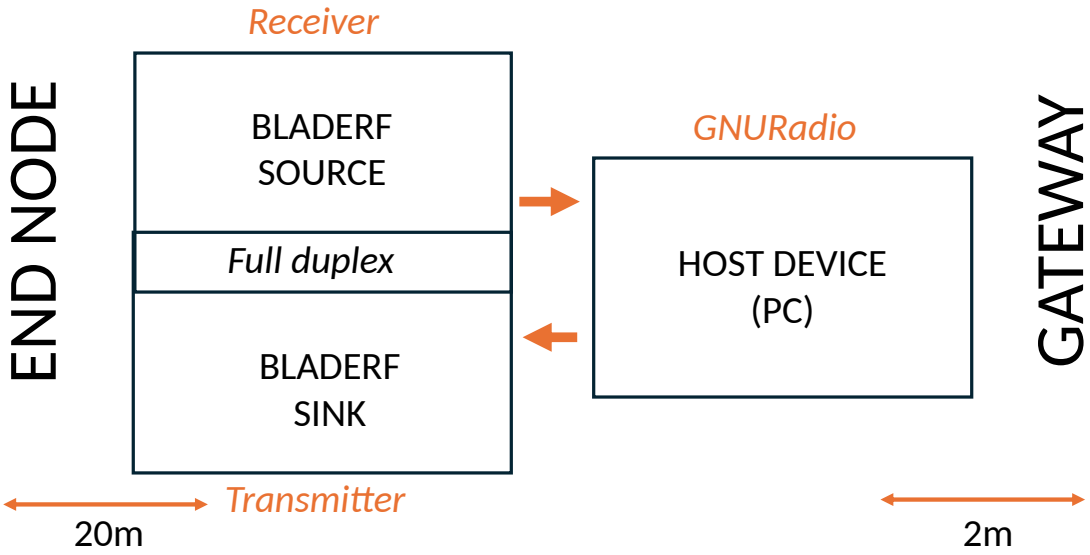

Figure 5. Scenario II block diagram setup.

Figure 6. Scenario II setup.

5.3. Step-by-Step Process: SCENARIO I

The step-by-step process for Scenario I is illustrated in Figure 7 and detailed in Algorithm 1.

- **Listening signal (process 1)**
  The system employs a structured listening process using a SDR and custom processing blocks to detect LoRaWAN packets with precision. The listening signal operates as a single process, which, through the Python multiprocessing library, shares events and data with a second process responsible for signal jamming. The SDR source, a bladeRF device, is configured to monitor

 doi:10.20944/preprints202503.0355.v1

signals within the 868.1 MHz band with a listening bandwidth of 2 MHz. This setup captures incoming radio signals, which are then analyzed through a series of ChirpDetector blocks, each calibrated for SF ranging from 7 to 12. These detectors identify LoRa chirps and provide key parameters such as the spreading factor, bandwidth, and normalized frequency.

A custom DetectionHandler block processes events triggered by the ChirpDetector blocks. It calculates the central frequency of the detected signal by using the normalized frequency output from the ChirpDetectors, along with the SDR's sampling rate and center frequency. Detected frequencies are then aligned to the nearest predefined LoRaWAN channel frequencies, such as 867.1 MHz or 868.3 MHz. When a valid chirp is detected, its parameters, including SF and frequency, are recorded, and a detection flag is raised to initiate subsequent processes, such as signal jamming.

The SDR source is connected in parallel to all ChirpDetector blocks, with detection events relayed to the DetectionHandler through message ports for real-time processing. This efficient architecture enables accurate detection and characterization of LoRaWAN packets, forming the foundation for advanced signal analysis and interference mechanisms.

- **Jamming signal (process 2)** The jamming process is implemented using a dedicated SDR and pre-recorded legitimate LoRaWAN packets for each SF. These precomputed signals are stored in memory and serve as inputs for the SDR sink, which is responsible for their transmission.

  When a valid detection is signaled by the detection flag, the system retrieves the detected SF and frequency from the first process. It then dynamically sets the frequency of the SDR sink to match the detected LoRaWAN signal. The system selects the appropriate pre-recorded and pre-loaded signal source corresponding to the detected SF and connects it to the SDR sink. Once the selection is complete, the flowgraph is started, initiating the jamming transmission.
- **Synchronization Between Processes**

  The sensing and jamming processes in the system are designed to run concurrently, leveraging Python's multiprocessing module to enable parallel execution and efficient synchronization. Multiprocessing provides a way to create separate processes that can execute tasks simultaneously, each with its own memory space. In the context of this system, multiprocessing is used to handle the independent operations of signal detection and jamming while ensuring they remain coordinated.

  Shared variables are a core feature of the multiprocessing framework, allowing real-time communication between processes. In this implementation, shared variables store key parameters such as the detected frequency and SF, ensuring both the sensing and jamming processes have consistent and accurate data. For instance, the detected frequency is updated by the sensing process and then accessed by the jamming process to adjust the transmitter's center frequency dynamically.

  In addition to shared variables, the system uses event flags to coordinate actions between processes. The detection flag signals the jamming process to start when a valid detection occurs. The jamming flag indicates when the transmitter is actively jamming, ensuring the sensing process pauses to avoid interference. The cooldown flag enforces a mandatory waiting period after jamming, preventing immediate consecutive detections and allowing the system to stabilize.

  By combining multiprocessing's ability to run parallel tasks with shared variables and event-driven synchronization, the system achieves real-time responsiveness and operational efficiency. This architecture ensures that the detection and jamming processes remain tightly integrated while operating independently, a critical requirement for time-sensitive signal processing tasks.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 March 2025 doi:10.20944/preprints202503.0355.v1

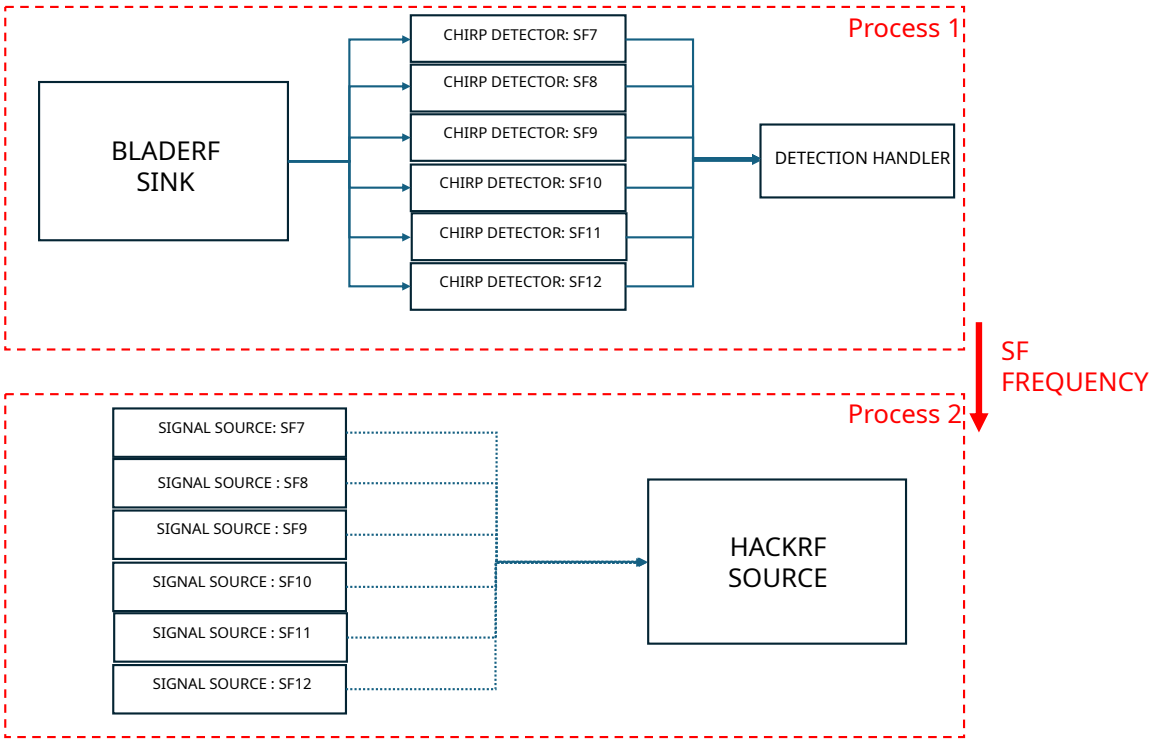

Figure 7. Block diagram of Scenario I.

Algorithm 1 Reactive Jamming - Scenario I

Process 1: Listening (BladeRF)
while *True* **do**
  `signal` ← READSIGNALFROMBLADERF(868.1 MHz, 2 MHz bandwidth)
  for `SF` in {SF7, SF8, SF9, SF10, SF11, SF12} **do**
    if CHIRPDETECTOR(`signal`, `SF`) == *True* **and not** jammingFlag **then**
      `frequency` ← CALCULATECENTERFREQUENCY(`signal`)
      `alignedFrequency` ← ALIGNFREQUENCYTOLORAWANCHANNEL(`frequency`)
      if `alignedFrequency` is valid **then**
        `detectedSF` ← `SF`
        `detectedFreq` ← `alignedFrequency`
        `detectionFlag` ← *True* {Signal jamming process}
      end if
    end if
  end for
end while
Process 2: Jamming (HackRF)
while *True* **do**
  if `detectionFlag` == *True* **then**
    `detectionFlag` ← *False*
    SETHACKRFFREQUENCY(`detectedSF`)
    `jammingPacket` ← SELECTPRERECORDEDJAMMINGPACKET(`detectedSF`)
    TRANSMITJAMMINGPACKET(`jammingPacket`, `HackRF`)
    `jammingFlag` ← *True*
    PACKET TRANSMISSION
    WAIT(`cooldownPeriod`)
    `jammingFlag` ← *False*
  end if
end while

 doi:10.20944/preprints202503.0355.v1

5.4. Step-by-Step Process: SCENARIO II

The step-by-step process for Scenario II is shown in Figure 8 and described in Algorithm 2.

- **Listening Signal**
  The listening process follows the same logic as described in Scenario I, utilizing the bladeRF SDR to capture and analyze LoRaWAN signals with high precision.
- **Jamming Signal**
  The jamming process is integrated within the same flowgraph used for signal detection, ensuring uninterrupted SDR operation. Since the parts of flowgraph cannot be dynamically turned on or off, a selector block is used to control the jamming mechanism. The selector dynamically switches between a pre-loaded jamming waveform and a zero-filled vector, allowing the bladeRF to transmit interference only when necessary while remaining active at all times.
  Upon detecting a LoRaWAN signal, the detection flag triggers the switching input of selector block. Initially, the selector block is set to the zero-filled vector (indicating no transmission). Once jamming is required, it dynamically switches to the appropriate jamming waveform for the detected SF. The bladeRF's transmitter aligns its center frequency to match the detected signal, ensuring accurate interference. After a predefined duration, the selector block is reset to the zero vector, halting jamming while keeping the flowgraph operational.
- **Signal Processing and Synchronization** Unlike Scenario I, this implementation operates within a single process, managing sensing and jamming sequentially. This reduces overhead and simplifies synchronization, while maintaining real-time responsiveness.
  Event flags coordinate the system's state transitions. The detection flag initiates jamming, temporarily pausing chirp detection to prevent interference with the transmitted signal. A cooldown period follows each jamming event, allowing the system to stabilize before resuming normal sensing operations.

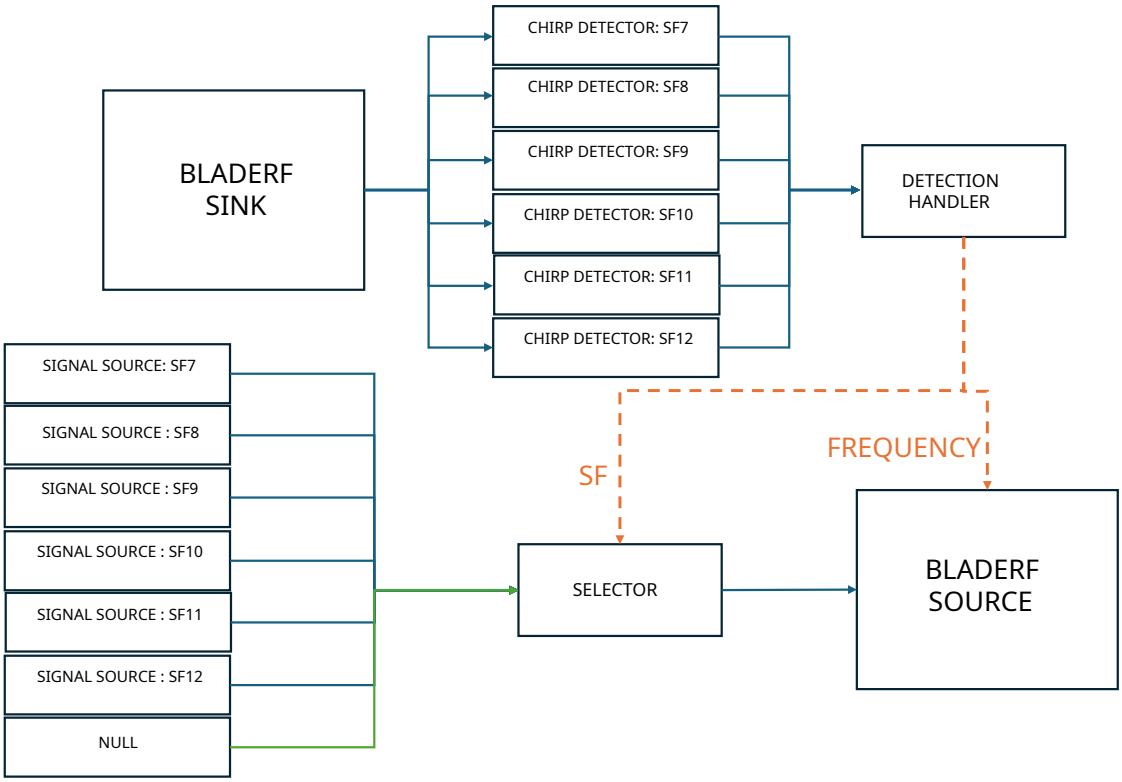

Figure 8. Block diagram of Scenario II.

 doi:10.20944/preprints202503.0355.v1

Algorithm 2 Reactive Jamming - Scenario II

```
while True do
  signal ← READSIGNALFROMBLADERF(868.1 MHz, 2 MHz bandwidth)
  for SF in {SF7, SF8, SF9, SF10, SF11, SF12} do
    if CHIRPDETECTOR(signal, SF) == True and not detectionFlag then
      frequency ← CALCULATECENTERFREQUENCY(signal)
      alignedFrequency ← ALIGNFREQUENCYTOLORAWANCHANNEL(frequency)
      if alignedFrequency is valid then
        detectionFlag ← True
        detectedSF ← SF
        detectedFreq ← alignedFrequency
        SETBLADERFTRANSMITTERFREQUENCY(detectedFreq)
        selectorBlock.switchInput ← jammingWaveform[detectedSF] {Switch to jamming waveform}
        WAIT(jammingDuration)
        selectorBlock.switchInput ← zeroFilledVector {Switch back to zero-filled vector}
        WAIT(cooldownPeriod)
        detectionFlag ← False
      end if
    end if
  end for
end while
```

6. Results

This section presents the experimental results obtained from implementing the reactive jamming attack on LoRaWAN networks in two distinct scenarios, as described in Section 5. The primary metric for evaluating the attack's effectiveness is the packet loss ratio (PLR), which indicates the percentage of packets successfully disrupted by the jamming attack. In addition, the reaction time distribution of the jammer is analyzed, highlighting differences in jamming performance between spreading factors.

6.1. Metrics Used to Measure Attack Effectiveness

The effectiveness of the reactive jamming attack was evaluated using two key metrics:

- **PLR**: Definition as the percentage of packets transmitted that were successfully jammed and did not reach their intended destination.
- **Reaction Time Distribution**: Analyzed using the Cumulative Distribution Function (CDF), which illustrates the probability that the jammer reacts within a certain time threshold.

These metrics provide insight into the attack performance under different experimental setups and spreading factors.

6.2. Experimental Setup and Methodology

Multiple trials were conducted for each experimental condition, covering all SFs and different payload sizes (1, 5, 15, and 20 bytes). Repeating the trials was essential to ensure statistical reliability of the results and to account for hardware-induced variations in reaction times.

- **Ensuring Reproducibility**: Given that SDR-based systems experience slight timing fluctuations due to processing delays, multiple trials helped confirm the consistency of attack effectiveness.
- **Comparing Different Scenarios**: Conducting multiple trials for Scenario I (HackRF One + BladeRF) and Scenario II (BladeRF only) ensured a fair comparison of the two setups.

For each SF, we transmitted and jammed 100 packets in varying payload sizes, and the PLR was measured for each condition. Reaction times were analyzed using the CDF to observe variations between trials. This approach ensured that our conclusions were robust, repeatable and statistically valid. Although the mean reaction time was used for a general comparison between Scenario I and Scenario II we relied on CDFs to visualize the probability of the jammer reacting within a specific time,

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 March 2025 doi:10.20944/preprints202503.0355.v1

clarifying reaction time differences across spreading factors. The transmitter, receiver and gateway were kept at a fixed distance to ensure that distance was not a factor in the results, and attention remained focused on synchronization rather than signal power.

6.3. Detailed Experimental Results

6.3.1. Power Spectral Density Analysis (PSD)

PSD of both the legitimate LoRaWAN signal and the jamming signal is shown in Figure 9. This plot highlights the frequency synchronization between the two signals, which is critical for effective jamming.

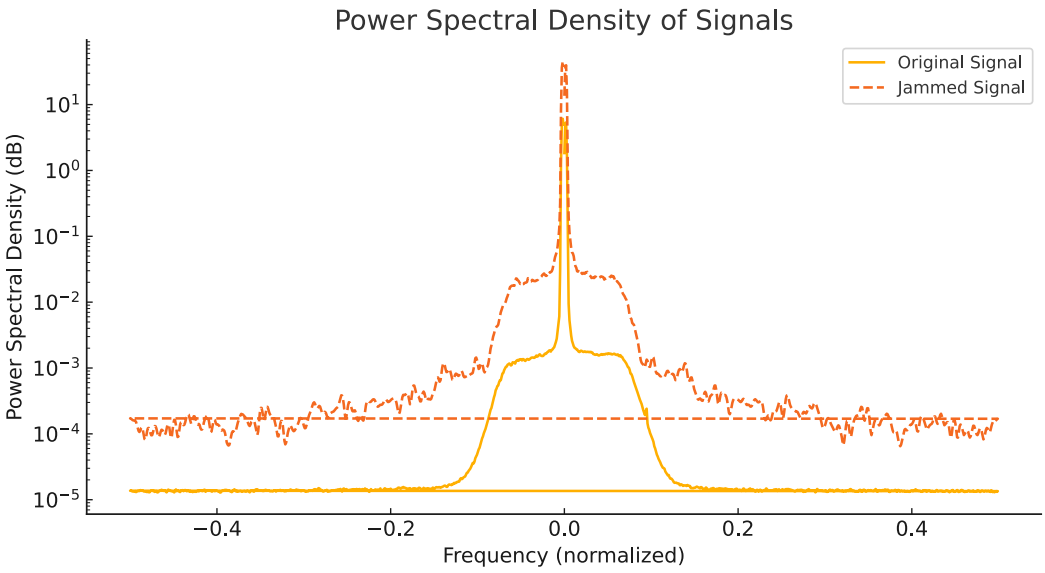

Figure 9. Power Spectral Density (PSD) of legitimate and jammed signals.

The PSD plot demonstrates the following:

- The jamming signal aligns closely with the center frequency of the legitimate LoRaWAN signal (normalized to 0), ensuring effective interference.
- The power level of the jamming signal is consistently higher than that of the legitimate signal on overlapping frequencies, effectively overpowering it.

This frequency synchronization is critical for successful jamming as it ensures that key portions of legitimate communication are disrupted. Without proper alignment frequency, the jammer would not effectively interfere with LoRaWAN transmissions.

6.3.2. Scenario I: BladeRF as Receiver, HackRF One as Transmitter

Figure 10 shows the spectrogram of a SF7 LoRaWAN jammed packet in Scenario I. Table 2 summarizes the PLR achieved in Scenario I. The results indicate a significant impact on LoRaWAN communication, with loss of packet 100% achieved across all spreading factors when the payload size was 5, 15, or 20 bytes. However, for a payload size of 1 byte, jamming was slightly less effective in SF7, where packet loss was 50%. Across all trials, payloads of five bytes or more incurred 100% packet loss, highlighting the power of reactive jamming.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 March 2025 doi:10.20944/preprints202503.0355.v1

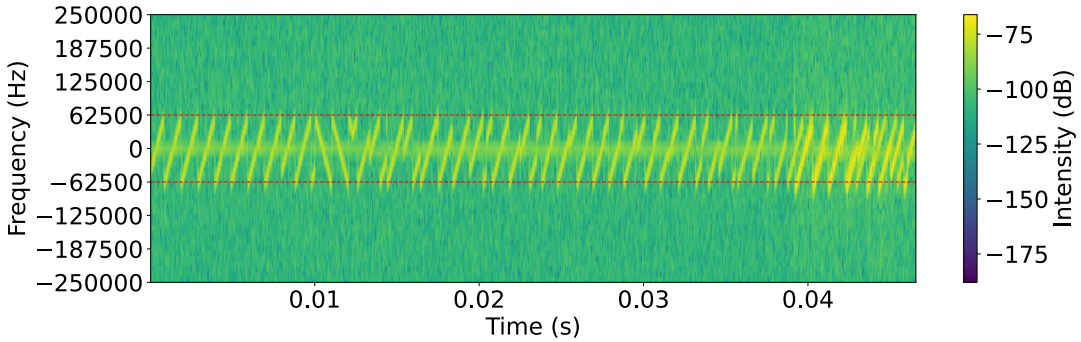

Figure 10. Scenario I: Spectrogram of SF7 LoRaWAN jammed packet(1 byte) on 868.1MHz center frequency.

Figure 12 provides additional insight into the attack performance by illustrating the duration of legitimate packets for each spreading factor and the percentage of overlap between legitimate and jamming packets. Higher overlap percentages indicate more effective jamming.

The reaction times of the jamming system in Scenario I are analyzed by the CDF graphs shown in Figure 14. The reaction times vary depending on the spreading factor, and lower SF values show faster reaction times because of shorter symbol durations. In Scenario I, reaction times varied slightly due to inter-device communication delays. This variability directly impacts the effectiveness of jamming, as shorter reaction times allow greater packet disruption.

Table 2. Scenario I

SF / Payload (Bytes)	1	5	15	20
SF7	50%	100%	100%	100%
SF8	100%	100%	100%	100%
SF9	100%	100%	100%	100%
SF10	100%	100%	100%	100%
SF11	100%	100%	100%	100%
SF12	100%	100%	100%	100%

6.3.3. Scenario II: BladeRF as Both Receiver and Transmitter

Figure 11 presents the spectrogram of an SF7 LoRaWAN jammed packet in Scenario II. Table 3 presents the PLR for Scenario II, where the reactive jamming attack proved universally effective. Unlike Scenario I, Scenario II achieved a 100% PLR across all SFs and payload sizes, demonstrating the advantage of using BladeRF for both receiving and transmitting.

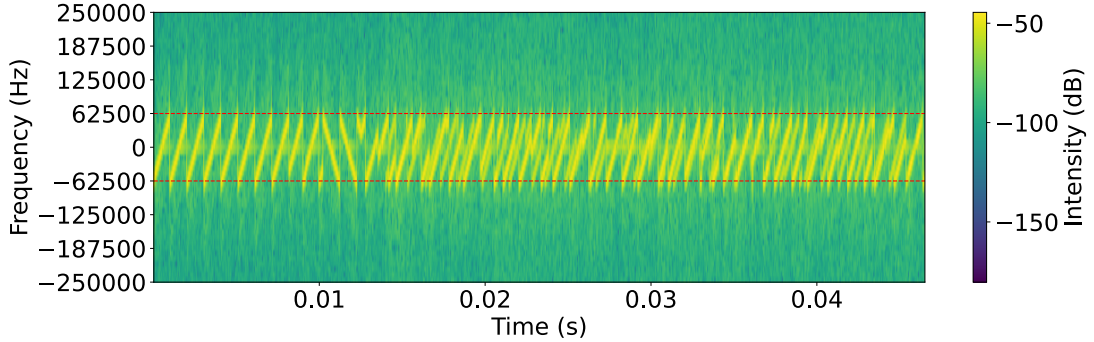

Figure 11. Scenario II: Spectrogram of SF7 LoRaWAN jammed packet(1 byte) on 868.1MHz center frequency.

Figure 13 illustrates the duration of legitimate packets and the percentage of overlap between legitimate and jamming packets. The streamlined single-device operation results in consistently high overlap percentages, explaining the superior jamming effectiveness in this scenario.

 doi:10.20944/preprints202503.0355.v1

The reaction times of the jamming system in Scenario II are also analyzed through the CDF graphs shown in Figure 14. Similar to Scenario I, the reaction times vary depending on the SF, with lower SF values showing faster reaction times due to shorter symbol durations.

Table 3. Scenario II

SF / Payload (Bytes)	1	5	15	20
SF7	100%	100%	100%	100%
SF8	100%	100%	100%	100%
SF9	100%	100%	100%	100%
SF10	100%	100%	100%	100%
SF11	100%	100%	100%	100%
SF12	100%	100%	100%	100%

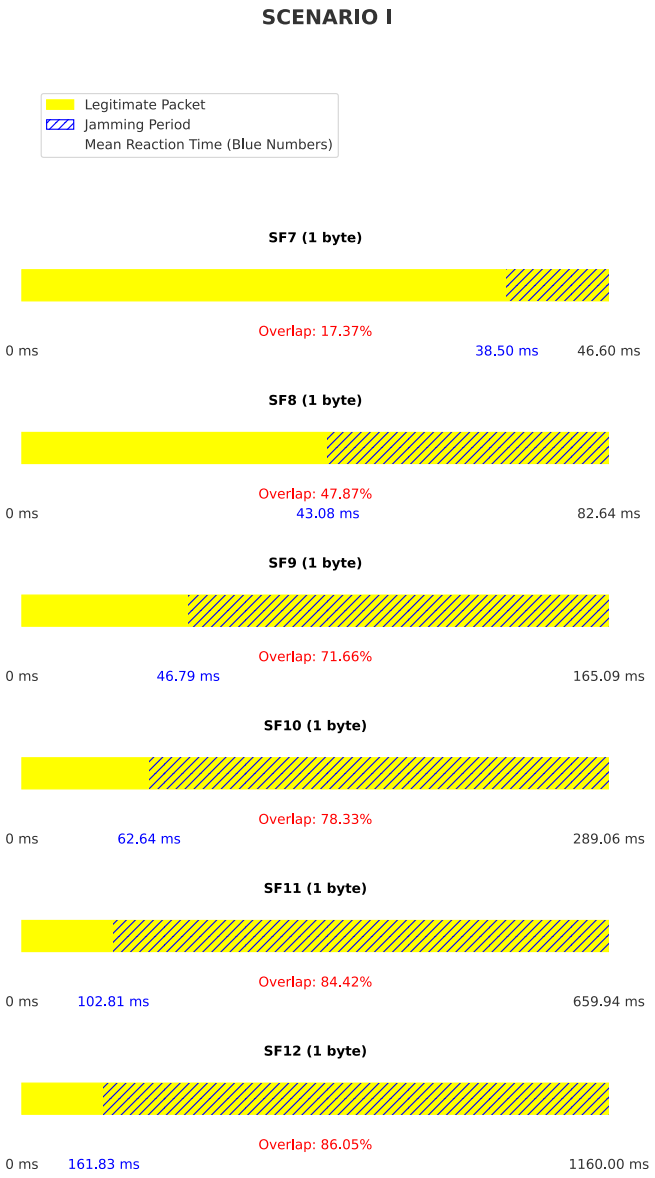

Figure 12. Results Scenario I.

 doi:10.20944/preprints202503.0355.v1

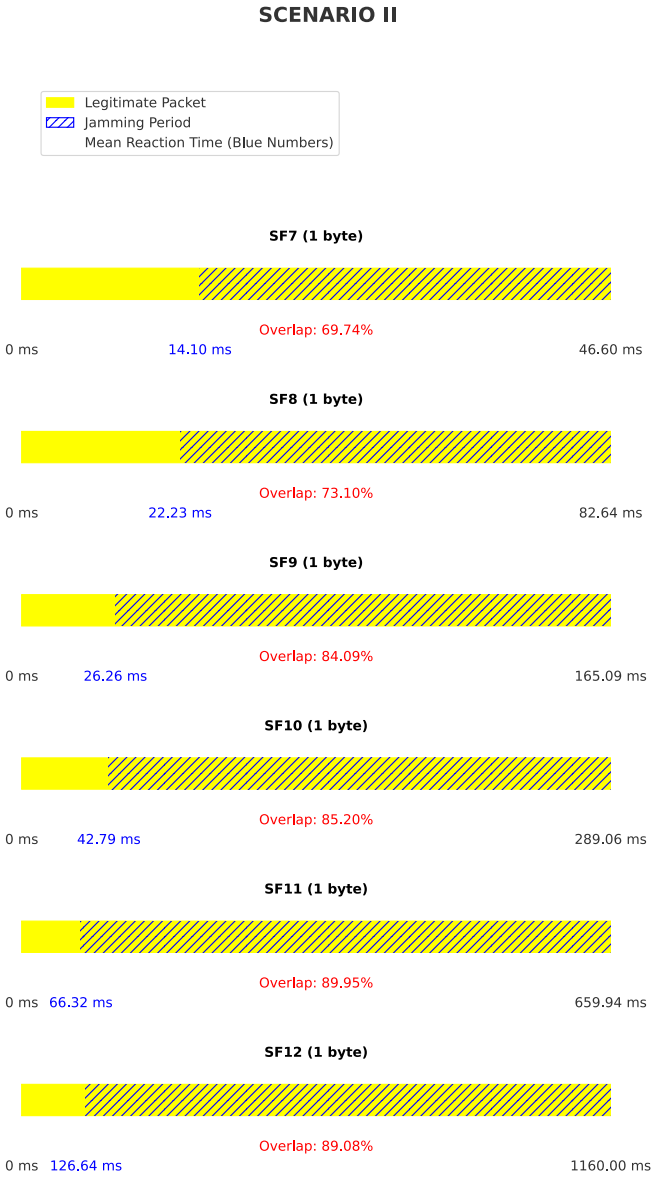

Figure 13. Results Scenario II.

 doi:10.20944/preprints202503.0355.v1

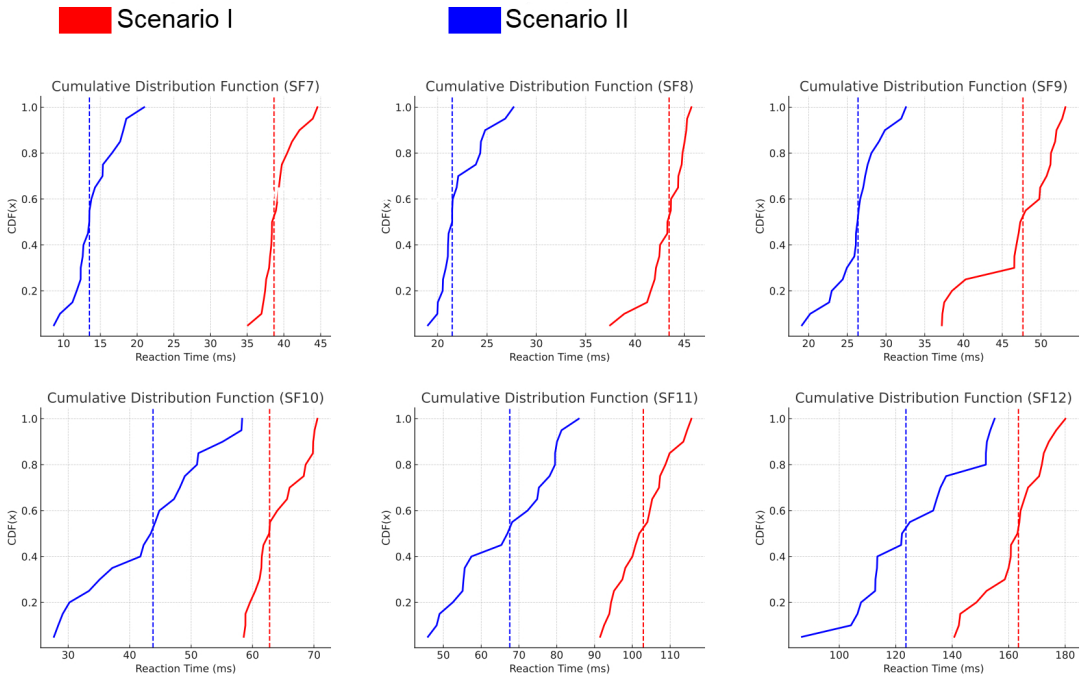

Figure 14. Cumulative Distribution Function of reaction time for each SF and scenario.

6.4. Limitations

The experimental setup was designed to isolate the impact of the reactive jamming attack on LoRaWAN networks, and care was taken to keep external parameters consistent in multiple trials. However, the evaluation does have some limitations, such as transmitter, receiver, and gateway being kept at a fixed distance to ensure that distance was not a factor in the results.

7. Discussion

The results of this study demonstrate the significant vulnerability of LoRaWAN networks to reactive jamming attacks, with both scenarios showing high effectiveness across different spreading factors and payload sizes.

7.1. Comparison of Scenarios

Scenario II, using a single BladeRF for both receiving and transmitting, proved to be more effective than Scenario I, which used separate devices for receiving (BladeRF) and transmitting (HackRF One). This difference is particularly notable for SF7 with 1-byte payloads, where Scenario I achieved only packet loss of 50% compared to 100% in Scenario II.

7.2. Jamming Effectiveness and Packet Overlap

Our findings confirm that reactive jamming success is strongly tied to how much the jamming signal overlaps the legitimate packet. Notably, for payloads of five bytes or more, both scenarios consistently yielded 100% packet loss.

Because partial overlap can invalidate the entire packet, LoRaWAN remains highly vulnerable to targeted interference. Future studies could explore the minimal jamming packet size needed for disruption and whether particular packet fields are more prone to attack.

7.3. Reaction Time and Spreading Factors

The CDF graphs show that reaction times vary with spreading factors:

- Lower SFs (e.g., SF7) exhibit faster reaction times due to shorter symbol durations.
- Higher SFs allow for longer reaction times while still achieving successful jamming because of larger duration of the packet.

 doi:10.20944/preprints202503.0355.v1

This variation in reaction times across SFs provides information on the time-sensitive nature of the LoRaWAN packet structure and the critical windows for effective interference.

7.4. Future Research Directions

1. **Minimal Jamming Packet Size**: Investigate the minimum size of jamming packets (e.g., few chirps) required for successful disruption.
2. **Targeted Jamming**: Analyze which specific parts of LoRaWAN packets are most vulnerable to jamming.
3. **Real-world Deployment Impact**: Assess the effectiveness of the attack in various environmental conditions and network topologies.
4. **Advanced Countermeasures**: Develop and test sophisticated defense mechanisms against reactive jamming.

This study underscores the urgent need for improved security measures in LoRaWAN networks, especially as IoT deployments continue to expand. The high success rate of jamming attacks, even with partial packet overlap, highlights a significant vulnerability that could potentially disrupt critical IoT applications that rely on LoRaWAN technology.

8. Conclusions

We implemented a practical reactive jamming attack on LoRaWAN using low-cost SDRs (HackRF One and BladeRF) under two experimental configurations. Both approaches severely disrupted LoRaWAN traffic across all spreading factors, reaching 100% packet loss in almost every case. In particular, a single device setup produced faster and more consistent jamming, underscoring the susceptibility of LoRaWAN to time-critical interference.

These findings highlight the inherent vulnerabilities of LoRaWAN when confronted with reactive jamming, particularly given LoRaWAN's reliance on unlicensed ISM frequency bands and its use of ALOHA-based medium access without robust collision avoidance mechanisms. Even partial overlap of legitimate and jamming signals was sufficient to prevent successful reception, underscoring the critical nature of precise timing and frequency alignment in attack execution.

Mitigating these vulnerabilities in LoRaWAN requires improvements at both the physical and network layers. Potential defenses include improved spread-spectrum techniques, dynamic channel hopping, or adaptive power and data-rate configurations. Furthermore, real-time jamming detection and proactive response strategies warrant focused research efforts.

As IoT applications relying on LoRaWAN continue to expand into mission-critical domains, addressing these security gaps becomes increasingly urgent. Future research directions should therefore focus on developing and rigorously testing countermeasures, such as early detection and mitigation algorithms, to maintain reliable, secure communication in large-scale IoT deployments.

Author Contributions: The individual contributions of each author are provided as follows: Conceptualization J.S and T.P.; methodology, J.S. and T.P.; software, J.S.; validation, T.P., J.S., P.S. and D.B.; formal analysis, J.S. and T.P.; investigation, J.S., T.P., P.S and D.B.; resources T.P. and P.S.; data curation, T.P and J.S.; writing–original draft preparation T.P. and J.S.; visualization T.P. and J.S.; supervision, P.S. and D.B.; project administration, P.S. and D.B.; funding acquisition, T.P. and P.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mahdavinejad, M.S.; Rezvan, M.; Barekatain, M.; Adibi, P.; Barnaghi, P.M.; Sheth, A.P. Machine learning for Internet of Things data analysis: A survey. *CoRR* **2018**, *abs/1802.06305*, [1802.06305].
2. Sain, M.; Kang, Y.J.; Lee, H.J. Survey on security in Internet of Things: State of the art and challenges. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), 2017, pp. 699–704. https://doi.org/10.23919/ICACT.2017.7890183.

 doi:10.20944/preprints202503.0355.v1

3. Sanchez-Iborra, R.; Cano, M.D. State of the Art in LP-WAN Solutions for Industrial IoT Services. *Sensors* **2016**, *16*. https://doi.org/10.3390/s16050708.
4. Centenaro, M.; Vangelista, L.; Zanella, A.; Zorzi, M. Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications* **2016**, *23*, 60–67. https://doi.org/10.1109/MWC.2016.7721743.
5. Mangalvedhe, N.; Ratasuk, R.; Ghosh, A. NB-IoT deployment study for low power wide area cellular IoT. In Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2016, pp. 1–6. https://doi.org/10.1109/PIMRC.2016.7794567.
6. Petäjäjärvi, J.; Mikhaylov, K.; Pettissalo, M.; Janhunen, J.; Iinatti, J. Performance of a low-power wide-area network based on LoRa technology: Doppler robustness, scalability, and coverage. *International Journal of Distributed Sensor Networks* **2017**, *13*, 1550147717699412.
7. Adelantado, F.; Vilajosana, X.; Tuset-Peiro, P.; Martinez, B.; Melia-Segui, J.; Watteyne, T. Understanding the Limits of LoRaWAN. *IEEE Communications Magazine* **2017**, *55*, 34–40. https://doi.org/10.1109/MCOM.2017.1600613.
8. Vangelista, L.; Zanella, A.; Zorzi, M. Long-Range IoT Technologies: The Dawn of LoRa™. In Proceedings of the Future Access Enablers for Ubiquitous and Intelligent Infrastructures; Atanasovski, V.; Leon-Garcia, A., Eds., Cham, 2015; pp. 51–58.
9. Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. A Survey of LoRaWAN for IoT: From Technology to Application. *Sensors* **2018**, *18*. https://doi.org/10.3390/s18113995.
10. Lora Alliance. LoRaWAN 1.1 Specification, Oct. 2017. http://lora-alliance.org/lorawan-for-developers. [Online; accessed 28-February-2021].
11. Mikhaylov, K.; Fujdiak, R.; Pouttu, A.; Miroslav, V.; Malina, L.; Mlynek, P. Energy Attack in LoRaWAN: Experimental Validation. In Proceedings of the Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019, ARES '19.
12. Butun, I.; Pereira, N.; Gidlund, M. Security Risk Analysis of LoRaWAN and Future Directions. *Future Internet* **2019**, *11*. https://doi.org/10.3390/fi11010003.
13. Yang, X.; Karampatzakis, E.; Doerr, C.; Kuipers, F. Security Vulnerabilities in LoRaWAN. In Proceedings of the 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), 2018, pp. 129–140. https://doi.org/10.1109/IoTDI.2018.00022.
14. Dönmez, T.C.; Nigussie, E. Security of LoRaWAN v1. 1 in backward compatibility scenarios. *Procedia computer science* **2018**, *134*, 51–58.
15. Butun, I.; Pereira, N.; Gidlund, M. Analysis of LoRaWAN v1.1 Security: Research Paper. 2018, SMARTOBJECTS '18.
16. Aras, E.; Small, N.; Ramachandran, G.S.; Delbruel, S.; Joosen, W.; Hughes, D. Selective Jamming of LoRaWAN Using Commodity Hardware. In Proceedings of the Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, 2017, MobiQuitous 2017, p. 363–372. https://doi.org/10.1145/3144457.3144478.
17. Aras, E.; Ramachandran, G.S.; Lawrence, P.; Hughes, D. Exploring the Security Vulnerabilities of LoRa. In Proceedings of the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), 2017, pp. 1–6. https://doi.org/10.1109/CYBConf.2017.7985777.
18. Noura, H.; Hatoum, T.; Salman, O.; Yaacoub, J.P.; Chehab, A. LoRaWAN security survey: Issues, threats and possible mitigation techniques. *Internet of Things* **2020**, *12*, 100303. https://doi.org/https://doi.org/10.1016/j.iot.2020.100303.
19. JungWoon Lee.; DongYeop Hwang.; JiHong Park.; Ki-Hyung Kim. Risk analysis and countermeasure for bit-flipping attack in LoRaWAN. In Proceedings of the 2017 International Conference on Information Networking (ICOIN), 2017, pp. 549–551. https://doi.org/10.1109/ICOIN.2017.7899554.
20. Yang, X. LoRaWAN: Vulnerability Analysis and Practical Exploitation. Master's thesis, Delft University of Technology, Delft, The Netherlands, 2017. M.Sc. Thesis.
21. Ingham, M.; Marchang, J.; Bhowmik, D. IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN. *IET information security* **2020**, *14*, 368–379.
22. Martinez, I.; Tanguy, P.; Nouvel, F. On the performance evaluation of LoRaWAN under Jamming. In Proceedings of the 2019 12th IFIP Wireless and Mobile Networking Conference (WMNC). IEEE, 9 2019, pp. 141–145. https://doi.org/10.23919/WMNC.2019.8881830.
23. Ahmar, A.U.H.; Aras, E.; Nguyen, T.D.; Michiels, S.; Joosen, W.; Hughes, D. Design of a Robust MAC Protocol for LoRa. *ACM Transactions on Internet of Things* **2023**, *4*, 1–25. https://doi.org/10.1145/3557048.

 doi:10.20944/preprints202503.0355.v1

24. Hou, N.; Xia, X.; Zheng, Y. Jamming of LoRa PHY and Countermeasure. *ACM Transactions on Sensor Networks* **2023**, *19*, 1–27. https://doi.org/10.1145/3583137.
25. Huang, C.Y.; Lin, C.W.; Cheng, R.G.; Yang, S.J.; Sheu, S.T. Experimental Evaluation of Jamming Threat in LoRaWAN. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring). IEEE, 4 2019, pp. 1–6. https://doi.org/10.1109/VTCSpring.2019.8746374.
26. José, A.N.D.S.; Deniau, V.; Gransart, C.; Vantroys, T.; Boé, A.; Simon, E.P. Susceptibility of LoRa Communications to Intentional Electromagnetic Interference with Different Sweep Periods. *Sensors* **2022**, *22*, 5015. https://doi.org/10.3390/s22135015.
27. Sun, Z.; Yang, H.; Liu, K.; Yin, Z.; Li, Z.; Xu, W. Recent Advances in LoRa: A Comprehensive Survey. *ACM Transactions on Sensor Networks* **2022**, *18*, 1–44. https://doi.org/10.1145/3543856.
28. Martinez, I.; Nouvel, F.; Lahoud, S.; Tanguy, P.; Helou, M.E. On the Performance Evaluation of LoRaWAN with Re-transmissions under Jamming. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC). IEEE, 7 2020, pp. 1–7. https://doi.org/10.1109/ISCC50000.2020.9219644.
29. Torres, N.; Pinto, P.; Lopes, S.I. Exploiting Physical Layer Vulnerabilities in LoRaWAN-based IoT Networks. In Proceedings of the 2022 IEEE 8th World Forum on Internet of Things (WF-IoT). IEEE, 10 2022, pp. 1–6. https://doi.org/10.1109/WF-IoT54382.2022.10152098.
30. Ahmar, A.U.H.; Aras, E.; Joosen, W.; Hughes, D. Towards More Scalable and Secure LPWAN Networks Using Cryptographic Frequency Hopping. In Proceedings of the 2019 Wireless Days (WD). IEEE, 4 2019, pp. 1–4. https://doi.org/10.1109/WD.2019.8734249.
31. Perković, T.; Rudeš, H.; Damjanović, S.; Nakić, A. Low-Cost Implementation of Reactive Jammer on LoRaWAN Network. *Electronics* **2021**, *10*, 864. https://doi.org/10.3390/electronics10070864.
32. Ruotsalainen, H. Reactive Jamming Detection for LoRaWAN Based on Meta-Data Differencing. In Proceedings of the Proceedings of the 17th International Conference on Availability, Reliability and Security. ACM, 8 2022, pp. 1–8. https://doi.org/10.1145/3538969.3543805.
33. Kalokidou, V.; Nair, M.; Beach, M.A. LoRaWAN Performance Evaluation and Resilience under Jamming Attacks. In Proceedings of the 2022 Sensor Signal Processing for Defence Conference (SSPD). IEEE, 9 2022, pp. 1–5. https://doi.org/10.1109/SSPD54131.2022.9896225.
34. Wadatkar, P.V.; Chaudhari, B.S.; Zennaro, M. Impact of Interference on LoRaWAN Link Performance. In Proceedings of the 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA). IEEE, 9 2019, pp. 1–5. https://doi.org/10.1109/ICCUBEA47591.2019.9128417.
35. Perkovic, T.; Siriscevic, D. Low-Cost LoRaWAN Jammer. In Proceedings of the 2020 5th International Conference on Smart and Sustainable Technologies (SpliTech). IEEE, 9 2020, pp. 1–6. https://doi.org/10.23919/SpliTech49282.2020.9243739.
36. Danish, S.M.; Nasir, A.; Qureshi, H.K.; Ashfaq, A.B.; Mumtaz, S.; Rodriguez, J. Network Intrusion Detection System for Jamming Attack in LoRaWAN Join Procedure. In Proceedings of the 2018 IEEE International Conference on Communications (ICC). IEEE, 5 2018, pp. 1–6. https://doi.org/10.1109/ICC.2018.8422721.
37. Dossa, A.; Amhoud, E.M. Impact of Reactive Jamming Attacks on LoRaWAN: a Theoretical and Experimental Study **2025**.
38. Šabić, J.; Perković, T.; Šolić, P. Chirp Detection and Signal Transmission: a HackRF Reactive Attack. In Proceedings of the 2024 International Conference on Smart Systems and Technologies (SST). IEEE, 10 2024, pp. 35–40. https://doi.org/10.1109/SST61991.2024.10755300.
39. Beltramelli, L.; Mahmood, A.; Österberg, P.; Gidlund, M. LoRa beyond ALOHA: An investigation of alternative random access protocols. *IEEE Transactions on Industrial Informatics* **2020**, *17*, 3544–3554.
40. Iglesias-Rivera, A.; Van Glabbeek, R.; Guerra, E.O.; Braeken, A.; Steenhaut, K.; Cruz-Enriquez, H. Time-slotted spreading factor hopping for mitigating blind spots in LoRa-Based networks. *Sensors* **2022**, *22*, 2253.
41. Gaitan, N.C. A long-distance communication architecture for medical devices based on LoRaWAN protocol. *Electronics* **2021**, *10*, 940.
42. LoRa Alliance Technical Committee. https://lora-alliance.org/resource_hub/lorawan-specification-v1-0-3/. [Online; accessed 28-February-2021].