Mitigating Jamming Attacks in LoRa Networks: A Defense Strategy against LoRa-Based Jammers

Md Ashikul Haque
University of Texas at Dallas

Abusayeed Saifullah
University of Texas at Dallas

Abstract

This paper addresses the vulnerability of LoRa communications against attackers transmitting LoRa packet and proposes an effective anti-jamming technique. Mitigating jamming in a LoRa network is extremely challenging as the devices have low computation power and limited energy. The state-of-the-art work addresses this type of jamming by exploiting Received Signal Strength Indicator (RSSI). It is effective only against a single jammer and is ineffective against multiple jammers transmitting LoRa packets with coordinated timing. The variability in arrival times of jamming LoRa packets results in differing RSSI, rendering the technique impractical against multiple jammers. In this paper, we propose a new technique to handle jamming when multiple attackers transmit LoRa packet simultaneously. Our idea is to implicitly synchronize all the LoRa symbols from different packets to ensure the jammers' energy in FFT bins remain distinguishable. This method is link layer-agnostic, entails no overhead at the LoRa nodes, and enables packet decoding even when facing attacks from a single jammer or multiple jammers on a channel, effectively combating reactive jamming. We have implemented our anti-jamming system at the LoRa gateway and conducted experiments under various jamming scenarios on LoRa nodes. The results show that our anti-jamming technique improves packet reception rate and per packet energy consumption by up to 106.56 and 135.15 times under collaborative jamming.

CCS Concepts

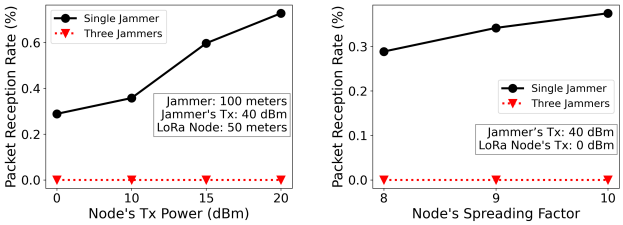
• **Security and privacy** → **Denial-of-service attacks**; *Mobile and wireless security*.

ACM Reference Format:

Md Ashikul Haque and Abusayeed Saifullah. 2025. Mitigating Jamming Attacks in LoRa Networks: A Defense Strategy against LoRa-Based Jammers . In *International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '25), October 27–30, 2025, Houston, TX, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3704413.3764442

1 Introduction

Jamming is a form of denial-of-service attack where malicious devices intentionally interfere with networks to obstruct legitimate communication. This type of attack has significant repercussions on wireless networks across economic, social, and military domains. In 2020, it was reported that 85% of cargo truck thefts in Mexico involved the use of wireless jamming [9]. Another notable instance occurred in March 2022, when SpaceX's Starlink system was subjected to a jamming attack [1]. Reliable communication is crucial during emergencies; however, jamming disrupts these communications, jeopardizing emergency responses and the exchange of critical information. Therefore, mitigating this threat to safeguard wireless communication is essential on both national and global levels.



(a) Varying Node's Tx Power (b) Varying Spreading factor

Figure 1: Performance of LoRa under severe jamming.

In this paper, we aim to strengthen LPWAN (low-power wide-area network) communications against wireless jamming attacks. LPWANs are designed for low-power, low data rate communication over long distances and are revolutionizing the IoT landscape. The demand for IoT applications is rapidly increasing, with an estimated 29 billion IoT devices projected by 2030 [40]. LoRa, a prominent LPWAN technology [2, 11], is deployed worldwide, with hundreds of millions of devices operating across all inhabited continents. LoRa supports over 600 use cases, including ship monitoring, asset anti-theft, vaccine temperature monitoring, and workplace CO_2 level monitoring [8]. According to ABI Research, LoRa is expected to account for over 50% of all LPWAN connections by 2026. The introduction of Long Range-Frequency Hopping Spread Spectrum (LR-FHSS) by Semtech further extends LoRa's coverage, potentially bridging terrestrial networks with low-earth orbit satellites to enable global low-power connectivity [3]. Given LoRa's extensive adoption and wide range of applications, we propose an anti-jamming technique specifically designed for LoRa.

LoRa faces increasing challenges from jamming due to its rapid expansion and widespread adoption, necessitating effective mitigation strategies. Because of its extensive coverage, LoRa signals can be detected over long distances, making them vulnerable to substantial jamming from multiple sources. A key vulnerability lies in the fact that jamming a small portion of the spectrum can disrupt numerous LoRa devices. Specifically, in LoRa networks, all end devices communicate directly with a gateway, making the gateway a single point of failure; jamming this point can incapacitate the entire network. Recent studies have shown that LoRa communications are susceptible to jamming attacks, resulting in significant packet loss, delays, and accelerated battery depletion [10, 32]. In our experimental investigation, illustrated in Figure 1, we observed that severe jamming reduces the packet reception rate from a LoRa node to below 1% with a single jammer and to 0% with multiple jammers, even when transmission (Tx) power and the spreading factor (a parameter that enhances LoRa reliability) are increased.

Mitigating jamming in a LoRa network is particularly challenging due to the devices' low computational power and limited energy, typically supplied by small, independent batteries. Existing research on LoRa primarily focuses on examining the impact of jamming [10, 22, 23, 32]. Several studies address packet collision issues or aim to decode signals under low interference power [13, 15, 31, 41, 42, 44, 45]. However, these techniques are unsuitable for mitigating jamming because the target LoRa signal quality can degrade significantly below the Signal-to-Noise Ratio (SNR) required for successful reception.

A recent study proposed in [20] addresses jamming by strategically positioning at least three gateways in a line and exploiting spatio-temporal offsets across these gateways. While effective against a single jammer, this method does not extend to multiple jammers. Similarly, [22] introduces a technique to combat jamming caused by a single jammer transmitting a LoRa packet. However, when multiple attackers simultaneously transmit LoRa packets for jamming, the variability in the arrival times of the jamming signals causes the energy to split across multiple FFT windows, rendering this technique ineffective.

In this paper, we propose a novel technique to mitigate the impact of multiple jammers that collectively transmit LoRa packets on the same channel to disrupt a LoRa network. The core concept of our approach is to synchronize the FFT windows of all LoRa packets—both jamming and legitimate—to ensure the jammers' LoRa symbols remain distinguishable. Upon identifying the FFT peaks caused by the jammers, these jamming LoRa symbols' FFT peaks are subtracted from the synchronized FFT windows. The proposed method is link-layer agnostic, introduces no additional overhead at the LoRa nodes, and enables successful packet decoding under attacks from both single and multiple jammers on the channel. This technique effectively counters reactive jamming.

We implemented our anti-jamming system on a LoRa gateway using a USRP (Universal Software Radio Peripheral) [6]. To evaluate its performance under various jamming scenarios, we conducted outdoor experiments with a deployment of ten LoRa nodes. Five of these nodes were based on Arduino boards [4] with LoRa shields [5], while the other five used Raspberry Pi boards with LoRa HATs incorporating the Semtech SX1276 LoRa transceiver. The results demonstrate that our technique improves packet reception rates by up to 106.56 times and decreases energy consumption per packet by up to 135.15 times compared to the baseline.

In the rest of the paper, Section 2 discusses related work. Section 3 provides an overview of LoRa, and Section 4 describes our jamming model. Section 5 introduces the problem and solution in high level, while Section 6 presents the detailed design of the anti-jamming system. Section 7 presents the experimental results. Section 8 concludes the paper.

2 Related Work

Many existing studies have explored the effects, detection, and mitigation of jamming in wireless networks [18, 36]. Most jamming mitigation techniques rely on spread spectrum methods, adaptive transmission (Tx) power, and frequency hopping [12, 30, 33, 35, 37, 38, 43], as well as coding-based approaches [34] and covert channel techniques [14]. While these methods can mitigate jamming to some extent, they are generally insufficient for handling severe or persistent jamming scenarios.

Some works have addressed collision recovery in wireless networks [16, 17, 24, 26–29]. mLoRa [42], FTrack [45], and CoLoRa [41] leverage either the temporal or spatial domain to resolve collisions in between LoRa packets. They cannot resolve collisions caused by other wireless signals and are not suitable for mitigating jamming as the jammers can send any jamming signal. Several studies propose to improve SNR for LoRa packet recovery by utilizing multiple gateways or nodes [13, 15], deep learning [31], or retransmitted packets [44]. However, these LoRa techniques can decode packets only when the SNR is at least -35 dBm. During jamming attacks, the SNR consistently falls below -35 dBm, rendering these techniques ineffective in handling jamming scenarios.

While jamming is a pervasive threat in wireless communications, mitigation techniques from other domains are often ill-suited for LoRa networks. LoRa's unique characteristics—namely its Chirp Spread Spectrum (CSS) modulation, low-power and resource-constrained nodes, and long symbol durations—render many conventional anti-jamming strategies ineffective or impractical. For instance, methods common in Wi-Fi or cellular networks like adaptive frequency hopping, dynamic power control, or complex MIMO beamforming are generally not feasible for LoRa devices due to hardware and energy limitations. Furthermore, LoRa's long symbol airtime makes it especially vulnerable to reactive jammers that can mimic its physical layer, a threat not addressed by general collision recovery schemes. Our work is therefore distinct as it targets this specific, structured interference model unique to LoRa, whereas other techniques are not designed for the high Signal-to-Noise Ratio (SNR) degradation caused by such malicious and tailored attacks.

Some recent studies have examined jamming and coexistence in LPWAN [19–23, 25, 32, 46]. The work in [46] focuses on jamming between the access point and the Internet. The studies in [10, 22] design jammers to disrupt LoRa communication. In [23, 32], the impact of jamming on LoRa networks is evaluated experimentally.

The work in [19] is designed to mitigate jamming from a single attacker in SNOW [39], and it is effective when the jammer follows their given game-theory model. To address jamming in LoRa from a single jammer, the approach in [20] proposes to decode packets by properly positioning at least three gateways in a line and by exploiting spatio-temporal offsets across the gateways. It is not applicable to multiple jammers, as the combined jamming signal differs at different gateways, making the technique unable to exploit any offsets.

[22] proposes a technique to mitigate synchronized LoRa jamming by exploiting differences in signal strength between jamming chirps and LoRa chirps. This approach is effective only when the jamming chirps are well-aligned with the LoRa chirps. Furthermore, it is designed to handle only a single jammer. In the presence of multiple attackers collectively transmitting jamming signals, variability in the arrival times of these signals causes the energy to split across multiple FFT windows, rendering this technique ineffective against multiple jammers transmitting LoRa packets.

In contrast, we propose a technique capable of decoding LoRa packets even when single or multiple reactive jammers collectively transmit LoRa packets of varying lengths on the same channel.

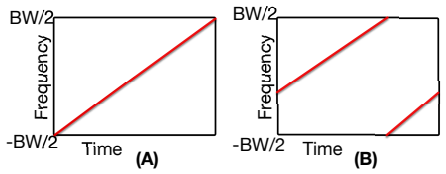


Figure 2: Illustration of modulation in LoRa: (A) The base up-chirp, or first symbol, is modulated by starting the frequency at the lowest value of its bandwidth and linearly increasing with time to the highest frequency in the bandwidth. (B) The base up-chirp is shifted to a different starting frequency to modulate a different symbol.

3 LoRa Overview

A LoRa system includes three components: gateway, end-devices (nodes), and network server. Nodes have limited computing power and energy, typically battery-powered, and communicate wirelessly with gateways. The gateway, powerful and line-powered, connects wirelessly to nodes and via IP connection to the network server, serving as a relay. The network server, possibly connected to multiple gateways, manages network parameters, security, and application requirements.

LoRaWAN is a MAC protocol for LoRa, similar to ALOHA. The LoRa band has separate uplink (node-to-gateway) and downlink (gateway-to-node) channels. LoRa employs Semtech's proprietary Chirp Spread Spectrum (CSS) modulation. LoRa transceivers feature five adjustable parameters: transmission power, carrier frequency, spreading factor (SF), bandwidth, and coding rate (CR). CR, ranging from 1 to 4, applies forward error correction to mitigate interference. SF values ($6 \leq s \leq 12$) define symbols encoded with 2^s chips, increasing SNR, sensitivity, and range at higher values.

Modulation. The CSS modulation is based on the manipulation of chirp signals. The fundamental chirp signal used is an *up-chirp*, where the frequency increases from the lowest frequency to the highest frequency in the bandwidth linearly over time as illustrated in Figure 2. This up-chirp serves as the base signal from which various symbols are derived. The symbols are created by shifting the frequency and duration of the base up-chirp. To create a symbol, the frequency of the up-chirp is shifted by a specific amount corresponding to the symbol's data content as depicted in Figure 2. Formally, a base up-chirp $C(k,t)$ is defined as:

$$C(k,t) = e^{j2\pi\left(\frac{1}{2}kt - \frac{BW}{2}\right)t}, \quad k = \frac{BW}{T},$$

where BW is the bandwidth and $T = \frac{2^{SF}}{BW}$ is the symbol duration. A LoRa symbol modulated at frequency offset f_{sym} can then be represented by:

$$S(f_{sym}, k, t) = C(k,t)e^{j2\pi f_{sym}t}.$$

Demodulation. LoRa demodulation begins with detecting the synchronization preamble at the start of a frame. The received up-chirp is multiplied by a corresponding *down-chirp* $C^{-1}(k,t)$, which is the complex conjugate of the base up-chirp. This multiplication transforms the chirped signal into a single tone:

$$S(f_{sym}, k, t)C^{-1}(k,t) = e^{j2\pi f_{sym}t}.$$

After applying a Fast Fourier Transform (FFT), the chirp's dispersed energy aggregates into a single frequency bin, enhancing the signal-to-noise ratio and enabling robust decoding even in low-power, noisy environments (Figure 3). Forward error correction (FEC) helps correct errors, and a Cyclic Redundancy Check (CRC) ensures data integrity.

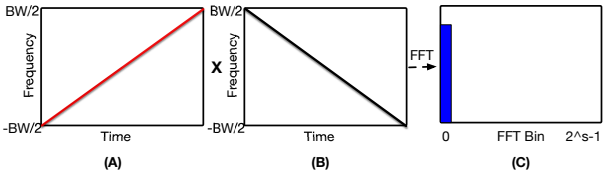


Figure 3: Illustration of symbol decoding in LoRa: (A) received signal in time domain; (B) multiplication of the signal with base down-chirp (highest frequency as starting frequency within the bandwidth); (C) after Fast Fourier Transform (FFT), energy accumulates into the starting frequency bin (e.g., bin 0 for the highest frequency), with the total bins determined by the spreading factor (s) as $2^s - 1$.

4 Jamming Model

Jamming disrupts communication by transmitting interfering signals on the same channel. In our model, multiple LoRa nodes communicate while facing potential *reactive jamming*. Reactive jammers detect legitimate transmissions and then interfere with them.

In our model, we focus specifically on attackers that transmit LoRa packets to disrupt communication. This focus is deliberate, as LoRa's CSS modulation is already robust against generic, unstructured noise, but it is highly vulnerable to structured interference that mimics its own modulation, especially when the spreading factor (SF) matches the legitimate signal. An attacker aiming to maximize disruption would logically choose this strategy. We consider a realistic scenario with a limited number of jammers per channel (e.g., up to four), as deploying more could bury the legitimate signal entirely, rendering technical defenses impractical. Furthermore, given that LoRa transmissions are often infrequent and have very long airtimes, reactive jamming is a far more practical and energy-efficient strategy for an attacker than constant or random jamming. This reactive nature is a crucial element of our threat model, as it creates the initial conditions that our defense mechanism exploits.

Since most LoRa communications are uplink (nodes to gateway), jammers primarily target these transmissions. Disrupting uplink packets prevents downlink acknowledgments (ACKs). Gateways, which can use higher power, are less susceptible to downlink jamming. Each jammer has an energy budget that influences its interference strategy. Although jammers can send long or consecutive packets, doing so incurs high energy costs. Given the sporadic nature of LoRa transmissions (few packets per hour per node), jammers must carefully time their interference to be effective.

In summary, our model examines reactive jammers that strategically disrupt uplink communication by coordinating the timing of their interference. Our goal is to develop robust anti-jamming techniques to protect these communications.

5 Mitigating Jamming from Multiple Coordinated Jammers in LoRa Networks

Jamming attacks in LoRa networks pose a significant threat to reliable communication, particularly when multiple jammers coordinate their timing. Existing techniques [20, 22] effectively mitigate

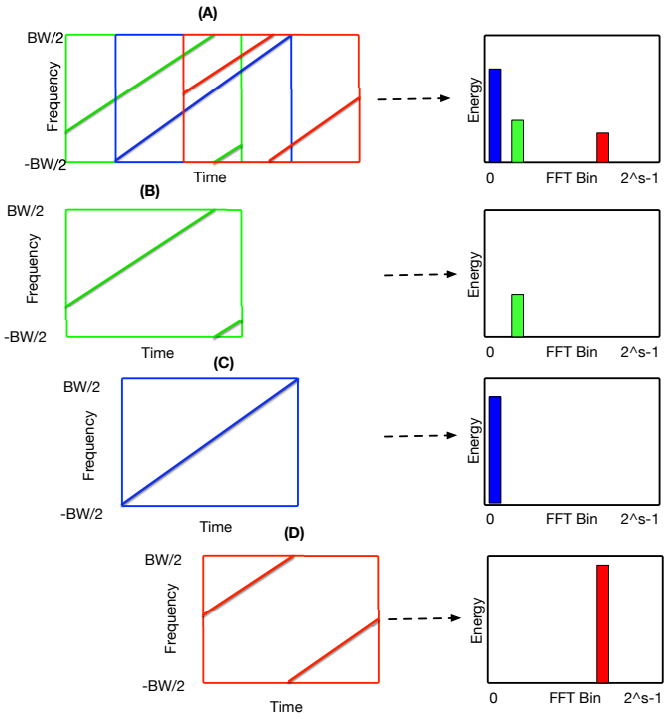


Figure 4: The challenge of multi-jammer interference with timing offsets. Subfigures (B), (C), and (D) show the ideal FFT energy for the legitimate signal and two jammers, respectively. Subfigure (A) shows how synchronizing to the legitimate signal's boundary in the combined signal causes the jammers' energy to scatter, distorting the FFT view.

interference from a single jammer but fall short when multiple jammers transmit on the same channel using the same SF. This section highlights the limitations of current jamming mitigation methods and introduces a novel approach that synchronizes incoming LoRa packets to counter the challenges posed by multiple coordinated jammers.

5.1 Understanding the Problem

Existing techniques for mitigating jamming in LoRa networks have primarily focused on scenarios involving a **single jammer**. For instance, the method proposed in [22] addresses jamming by detecting and subtracting the jammer's energy peak in the FFT window to isolate the legitimate LoRa symbol's energy peak. When only one jammer is present, and the legitimate LoRa packet and the jamming signal are synchronized, this technique is effective because the jamming signal maintains a consistent Relative Signal Strength Indicator (RSSI) across FFT windows. However, these techniques are insufficient for handling multiple jammers due to coordinated timing.

Figure 4 illustrates this core challenge by contrasting the ideal energy representation of individual signals with the distorted view seen in a combined, misaligned scenario. Subfigures (B), (C), and (D) show the legitimate signal (green) and two progressively stronger jammers (blue and red), each analyzed within its own ideal symbol window. In these isolated views, their respective energy peaks in the FFT are clear and proportional to their true signal strength.

Subfigure (A), however, depicts the realistic problem at the gateway. It shows the FFT of the combined signal, but the demodulation window is synchronized only to the boundary of the legitimate signal shown in (B). Because the jamming signals from (C) and (D) arrive with a temporal offset, their symbols are misaligned with this window. This causes their energy to be improperly integrated and scattered across multiple FFT windows. The result is a highly deceptive energy profile: the blue jammer's peak is diminished but still overwhelms the legitimate one, while the strongest jammer's peak from (D) is now the smallest in the window. Any defense based on simple RSSI filtering would fail in this scenario, as it cannot correctly identify the true strength and presence of all jammers.

Multiple jammers using the same spreading factor (SF) present a fundamentally different challenge. Theoretically, if the legitimate symbol is modulated as:

$$S(f_{sym}, k, t) = C(k, t)e^{j2\pi f_{sym}t},$$

then multiple jamming signals modulated with different frequency offsets $f_{sym,j}$ and time offsets cause energy dispersion according to:

$$S(f_{sym,j}, k, t + \Delta t_j)C^{-1}(k, t) = e^{j2\pi[f_{sym,j}(t+\Delta t_j)+\frac{1}{2}k(\Delta t_j)^2]},$$

where Δt_j is the temporal offset of the jammer's symbol. This causes energy scattering across FFT bins.

In practical scenarios, jammers exploit LoRa's inherent vulnerability by transmitting jamming signals with the same SF as the legitimate LoRa node. This synchronization in SF is critical because LoRa transmissions with different SFs are orthogonal and do not interfere with each other [47]. If jammers used a different SF, their attempts to disrupt the legitimate signal would fail. Therefore, to maximize their disruptive impact, multiple jammers typically coordinate to use the same SF as the target LoRa node. This coordination exacerbates the challenge, as their collective interference becomes harder to mitigate.

When multiple jammers' transmissions are synchronized, their signals can create distinct high-energy peaks in FFT bins, making it possible to apply the technique in [22] to mitigate the jamming effect. However, it is more effective for jammers to coordinate their timing to avoid full synchronization while still transmitting simultaneously. After detecting a legitimate LoRa packet, the jammers ensure their signals arrive at the gateway with temporal offsets. This strategy causes their energy to be distributed across different FFT windows. Consequently, the method in [22] fails to consistently detect the dominant energy peaks contributed by the jammers, rendering existing techniques ineffective.

5.2 Proposed Solution

To address the limitations of existing techniques, we propose a novel approach that involves the implicit synchronization of all incoming LoRa packets' symbols. This synchronization ensures that the energy from multiple jamming signals does not split into different FFT bins, thereby facilitating accurate jamming mitigation and symbol decoding.

Each LoRa packet begins with a preamble (n base up-chirps), followed by the Start Frame Delimiter (SFD) (2.25 base down-chirps), which marks the start of the payload data. The preamble consists of a series of up-chirps, while the SFD introduces a distinct contrast

by transitioning from an up-chirp to a down-chirp. This contrast in the SFD enables precise detection of the symbol window, even when signal energy levels vary significantly.

The proposed solution begins by detecting the preamble and SFD of each incoming signal. Despite significant energy discrepancies between the legitimate LoRa signal and the jamming signals, the gateway can detect these signals by accumulating energy over multiple symbol windows. This accumulation increases the likelihood of detecting the weaker legitimate signal amidst stronger jamming signals. The approach also effectively manages the computational load, ensuring efficient processing of multiple signals.

Once a signal is detected through its preamble, the SFD is used to identify the exact symbol boundary. The transition from an up-chirp to a down-chirp in the SFD provides a reliable marker for delineating the symbol boundary. After detecting the symbol boundary of one signal, the gateway processes other incoming signals in parallel. This parallel processing ensures that all LoRa packets on the channel—both legitimate and jamming—are detected, and their symbol windows are identified.

After detecting the symbol windows of all incoming LoRa packets, the gateway synchronizes these symbols by aligning them based on their symbol boundaries. Following synchronization, the gateway aggregates the energy contributions from the jamming LoRa symbols and isolates them from the legitimate LoRa symbol. The synchronized jamming LoRa symbols' energy can then be subtracted from the combined signal, enabling accurate decoding of the legitimate LoRa symbol.

Mathematically, symbol demodulation using FFT is given by:

$$\text{FFT}\{S(f_{sym}, k, t)C^{-1}(k, t)\} \rightarrow \text{Peak at bin } f_{sym}.$$

Misalignment of FFT windows disperses symbol energy. The synchronization approach aligns symbol windows to ensure:

$$\text{FFT}\{S(f_{sym,j}, k, t)\} \approx \text{Single peak at bin } f_{sym,j}, \quad \forall j,$$

isolating jammer symbols from legitimate symbols effectively.

In summary, the proposed technique addresses the challenge of jamming from multiple coordinated jammers by: 1) Detecting incoming LoRa packets, 2) Processing signals in parallel and identifying their symbol windows, and 3) Synchronizing the detected symbol windows to prevent the dispersal of jamming energy across FFT bins.

The extraction of actual signal as shown in Figure 4 (B,C,D) is not possible with any existing technique. So how can we synchronize them while they remain in combined form.

Implementing this solution poses major challenges, such as aligning signals already in combined form and isolating the FFT peaks contributed by the jammers. We will address these challenges and design a system to decode legitimate LoRa symbols effectively.

6 System Design

The proposed jamming mitigation technique is implemented by modifying a traditional LoRa decoder system by incorporating specialized modules designed to address the challenges posed by multiple jammers. The workflow is depicted in Figure 5, where the colored blocks are contribution of this work. The architecture consists of four primary modules, each fulfilling a specific function to ensure the accurate decoding of legitimate LoRa signals, even under adversarial conditions. Together, these modules facilitate real-time processing, precise synchronization, and reliable mitigation of jamming.

The modular design provides distinct advantages. By decoupling the tasks of signal acquisition, boundary detection, demodulation, and decoding, the system can be easily adapted or upgraded to accommodate new jamming techniques or variations in LoRa transmission protocols. Each module operates independently-allowing parallel processing, significantly enhancing the system's ability to handle high-throughput environments where numerous legitimate and jamming signals may coexist.

6.1 LoRa Packet Detection

This module serves as the initial stage of the system, continuously monitoring the LoRa communication channel for incoming signals. It performs real-time detection and processing to ensure no signal, whether legitimate or jamming, is overlooked. The module scans the channel for the presence of LoRa-specific preambles, which are sequences of up-chirps characteristic of LoRa transmissions.

In typical LoRa implementations, detection relies on identifying n continuous base up-chirps, where n is determined by the network configuration. To enhance detection reliability, we sum the FFT bin energies of n consecutive windows. If, after summation, any bin's energy exceeds a predetermined threshold, the system considers a LoRa packet to be incoming and begins saving the signal for future processing.

Crucially, this detection process leverages the reactive nature of the jammers. Jammers must first detect a legitimate transmission before they can begin their own, a process which itself takes time. This typically provides a brief, interference-free window where the legitimate LoRa preamble arrives at the gateway alone. This initial, clean reception is essential for the gateway to detect the packet's existence and establish its baseline Received Signal Strength Indicator (RSSI) before the jamming signals arrive and corrupt the channel. After this initial detection, the system begins saving the raw signal to ensure the subsequent Start Frame Delimiter (SFD) and payload are captured for processing.

After detecting an incoming LoRa packet, the system reverts to the standard LoRa detection mechanism. This step prevents false detections while a LoRa packet is already being received. When the module detects a LoRa packet using the proposed mechanism, it starts saving the raw signal received from the channel, along with a timestamp.

6.2 Symbol Boundary and RSSI Determination

This module processes the signals saved by the previous module and determines the symbol boundaries for each detected signal. This is accomplished by leveraging the SFD, which provides reliable markers for symbol alignment. The preamble consists of a series of up-chirps, while the SFD contains a distinct transition to a down-chirp. This feature allows for the precise localization of symbol boundaries, even in the presence of noise or interference.

The raw signal saved by the previous module contains both the preamble and SFD because it preemptively starts saving the signal before detection. If no incoming LoRa packet is detected, the preemptively saved signals are discarded. This module uses

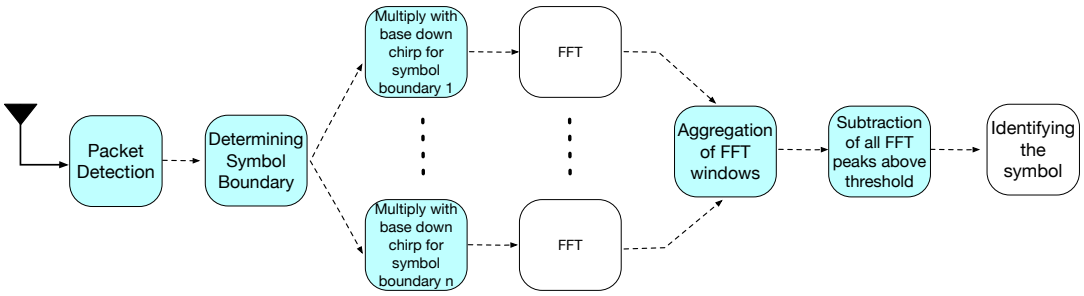


Figure 5: Illustration of workflow in anti-jamming decoder.

the usual LoRa symbol boundary detection, which relies on the length of the 2.25 base down-chirp in the SFD. This straightforward approach works for the legitimate LoRa packet since it typically does not get interfered with by the jammers' LoRa packets at this stage due to the jammers' reactive nature.

Detecting the jammers' symbol boundaries is more challenging. If the jammers' packets arrive almost simultaneously, precise boundary detection becomes difficult. However, in such cases, a single symbol boundary can be used for all jammers' packets. Even though this approximates the boundary for all jammers' packets, it is usually sufficient to detect the distinct energy peak in the FFT window because only a small amount of energy spills into adjacent FFT windows.

If the jammers' packets arrive at different times, the contrast change from base up-chirp to base down-chirp in each jammer's LoRa packet can be exploited to determine the start of the SFD. Using the prior knowledge that the jammers are using the same SF as the legitimate LoRa packet, the other side of the symbol boundary can be determined. This works because symbols with the same SF have the same symbol length.

Using the techniques mentioned above, this module determines the symbol boundary for the legitimate LoRa packet and all jamming LoRa packets. While detecting the boundary, this module also determines the RSSI for the legitimate LoRa packet. It first calculates the RSSI of the legitimate LoRa packet before it has been interfered with. This is done by analyzing the packet's energy levels in the FFT window for all the base up-chirps in the preamble and the base down-chirps in the SFD to establish the RSSI trend for the legitimate LoRa packet.

6.3 Parallel Demodulation

This module is the core of the system, designed to address the complexities of multiple coordinated jammers. Unlike traditional LoRa decoders that demodulate using a single base down-chirp, this module performs demodulation operations concurrently for each detected signal, including both legitimate and jamming signals. If there are n detected signals, the module executes n parallel demodulation operations, where $n-1$ signals typically correspond to jammers.

Upon receiving the n copy of the combined signal and the corresponding symbol boundaries, the module segments the signals based on their boundaries. For each segment, it multiplies the signal by base down-chirp to de-spread it. The FFT is then applied to each demodulated segment, producing n distinct FFT windows, each representing the frequency-domain characteristics of one of the detected signals.

These n FFT windows are not synchronized and if we synchronize them it means we are actually synchronizing the symbols of different LoRa packet according to their symbol boundary. We know that same symbol of a LoRa packet will contribute differently to all these n FFT windows. Suppose we are considering the i-th LoRa packet's first symbol s_{i1}, the contribution of energy by s_{i1} across FFT windows $(1,\ldots,i,\ldots,n)$ can be written as $E_{s_{i1}} = (e^1_{s_{i1}},\ldots,e^l_{s_{i1}},\ldots,e^n_{s_{i1}})$. Here, each symbol's energy contribution in FFT window l is:

$$e^l_{s_{ij}} = \left|\text{FFT}\{S(f_{s_{ij}},k,t+\Delta t_{il})C^{-1}(k,t)\}\right|^2,$$

where Δt_{il} is the symbol boundary offset.

These are essentially the copy of the s_{i1}'s energy where the boundary is different across different FFT windows — resulting in different values in members of $E_{s_{i1}}$. Now, if we think carefully, the highest value in $E_{s_{i1}}$ will be $e^l_{s_{i1}}$, meaning i's own FFT window where the entire symbol's energy is getting accumulated into its FFT bin. In other FFTs, all the energy is not getting accumulated; rather, a portion of it is getting accumulated depending on the overlap between its symbol boundary and others' symbol boundaries. Mathematically, we can write this as:

$$e^{sync}_{s_{ij}} = \max_{1\le l\le n}(e^l_{s_{ij}}).$$

In summary, if we take all n FFT windows and symbols, and in a separate FFT window for each symbol only take the highest energy peak across all n FFT windows, we will end up with an aggregated and synchronized FFT window where all the symbols have their own FFT window's energy. This means we have essentially synchronized them in the FFT level, which is analogous to synchronizing them in the time domain by shifting individual signals and matching their symbol boundaries (which was not possible as we could not disentangle them from the combined signal). But in this manner, we might override our legitimate LoRa symbol with a jamming LoRa symbol due to the jamming LoRa symbol being the same and having higher energy in the FFT bin.

That's where we add a safeguard and check symbols' energy in the FFT bins having similar RSSI (obtained from the previous module) as our legitimate LoRa packet. If any symbol has energy in an FFT bin similar to our legitimate LoRa packet's RSSI, it will have the highest priority, and its FFT bin's energy will not be replaced

in the aggregate FFT bin. This does not guarantee success in every case, but it increases our probability of successful decoding.

This process of creating an aggregate FFT window by selecting the maximum energy contribution for each symbol across all n demodulation paths serves as a form of implicit synchronization. While the combined signal cannot be separated in the time domain, this frequency-domain technique achieves an analogous result. Each of the n parallel FFT operations is aligned with a different signal's symbol boundary. A symbol's energy will be maximally concentrated into a single FFT bin only in the window that is perfectly aligned with its own boundary. In all other misaligned windows, its energy will be scattered. Therefore, by taking the maximum peak value for each symbol across all windows ($e^{sync}_{s_{ij}} = \max_{1 \le l \le n}(e^{l}_{s_{ij}})$), we are effectively reconstructing a synchronized FFT view where each symbol, whether legitimate or jamming, is represented as if it were demodulated in its own ideal time window. This allows us to mitigate the energy-splitting effects caused by timing offsets without requiring physical signal separation.

6.4 Decoding

This module receives the implicitly synchronized LoRa symbols' aggregate FFT window. It processes this FFT window and decodes the legitimate LoRa packet's symbol. Using the legitimate LoRa packet's RSSI, it isolates the FFT peak contributed by the legitimate LoRa packet's symbol, enabling successful decoding.

From the module in Section 6.2, this module obtains the RSSI of the legitimate LoRa packet. It then uses this value as a threshold with some margin m (m is a hyperparameter). Any FFT bin with a value greater than RSSI + m is set to zero. This process is analogous to eliminating all FFT peaks other than those of the legitimate LoRa symbol. Since jamming LoRa symbols typically have higher energy peaks than the legitimate LoRa symbol, this step effectively removes all FFT peaks contributed by the jamming LoRa symbols.

At this point, we are left with an FFT window containing only the FFT peak attributed to the legitimate LoRa symbol. Therefore, we can decode the legitimate LoRa symbol corresponding to this FFT peak.

6.5 Summary

The system continues running the demodulation and decoding module until the entire legitimate LoRa packet has been decoded. Based on prior knowledge, the system knows how many symbols are needed to fully decode the packet. Therefore, the system repeats this process x times if there are x symbols in the legitimate LoRa packet. After that, any symbols from jamming LoRa packets are discarded.

The proposed system design integrates the jamming mitigation technique into a conventional LoRa decoder by introducing several key functionalities. The *LoRa Packet Detection* module detects and captures incoming LoRa packets with timestamps in real-time, ensuring that no signal is missed. The *Symbol Boundary and RSSI Determination* module identifies the boundaries of each signal, facilitating precise synchronization. The *Parallel Demodulation* module demodulates all detected signals concurrently, addressing the challenges posed by multiple jammers. Finally, the *Decoding* module isolates the legitimate LoRa symbol by discarding high-energy jamming peaks.

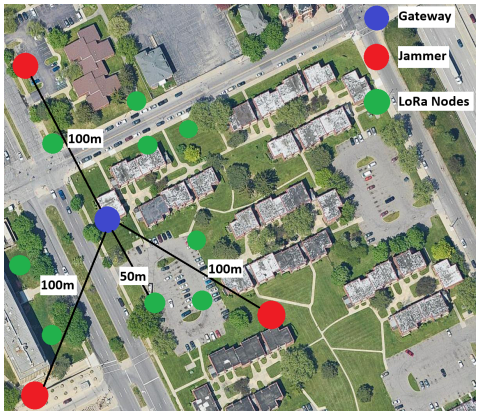


Figure 6: Default Setup.

This comprehensive approach enhances the resilience and reliability of LoRa networks. By combining real-time processing, accurate synchronization, and robust interference mitigation, the system ensures reliable communication even in the presence of multiple jammers transmitting LoRa packets simultaneously. The modular design allows for scalability and adaptability, making it suitable for deployment in a wide range of LoRa network environments.

7 EXPERIMENTS

This section presents the setup and result of the experiment to evaluate our proposed anti-jamming system.

7.1 Setup

We conduct the experiment outdoors in a suburban metropolitan area using four USRP B200s [6] implemented in GNU Radio [7]. These serve as one LoRa gateway and three jammers. For the LoRa node, we utilize five Dragino LoRa shield [5] paired with an Arduino Uno R3 [4] and five Raspberry Pi with LoRa HATs based on the SEMTECH SX1276 LoRa transceiver. The jammers are reactive in all setups.

In all setups, the LoRa nodes operate on separate channels between 902-915 MHz with a spreading factor of 8 (except in varying-SF configurations), a bandwidth of 125 kHz, and a coding rate of 4/5. Performance is evaluated using 1000 packets transmitted every 10 seconds, each sized at 32 bytes. Jammers transmit 64-byte packets at any SF. Default transmission powers are 10 dBm for LoRa nodes and 30 dBm for jammers. The jammers collectively jam one channel at a time meaning one node is affected by the jammers in this setup. The setup, shown in Figure 6, is consistent across all experiments, with variations only in distance and the number of jammers. Experiments are repeated multiple times, repositioning jammers on a circular path with a radius matching the specified distance. We compare our approach with state-of-the-art anti-jamming techniques for LoRa, specifically baseline [22] and baseline 2 [20].

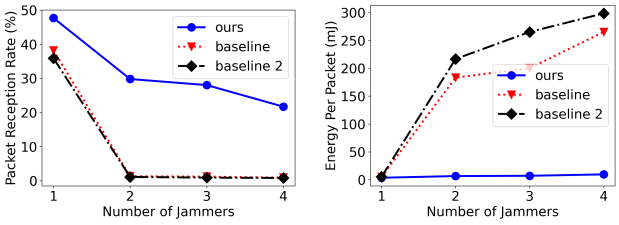
7.2 Experimental Result

For evaluation, we use two metrics: Packet Reception Rate (PRR) and Energy Per Packet (EPP).

- PRR is calculated as $\text{PRR} = \frac{\text{Total Received Packets}}{\text{Total Transmitted Packets}}$.
- EPP is calculated as $\text{EPP} = \frac{\text{Total Energy for Transmission + Total Energy for Retransmission}}{\text{Total Received Packets}}$.

Note that a higher PRR and lower EPP indicate better performance. In all results, we calculate the metrics only for nodes experiencing jamming attacks. To present unbiased results, we exclude packet transmissions from unjammed nodes. Our metrics calculations rely on the MAC layer, which employs Cyclic Redundancy Check (CRC) for error detection. If symbol errors exceed the threshold set by the coding rate, the packet is discarded due to incorrect reception.

7.2.1 Varying Number of Jammers. In this setup, we vary the number of jammers from one to four and measure the metrics. We run this experiment for another existing technique [20] designed for single jammer.

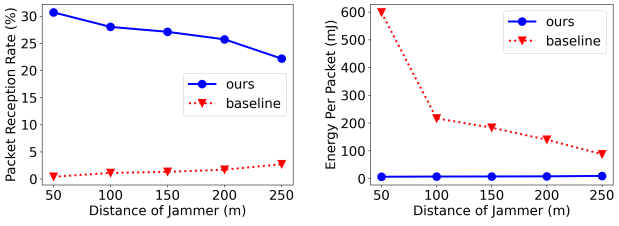


(a) Packet Reception Rate (b) Energy Per Packet

Figure 7: Performance varying number of jammers.

As illustrated in Figure 7, both PRR and EPP remains very low for baseline and baseline 2 [20] when the number of jammer is more than one. When the number of jammer is one, the baseline outperforms baseline 2 by a slight margin due to it being specially designed to work against jammers transmitting LoRa packets. Even though baseline and baseline 2 performs competitively when the number of jammer is one, our approach outperforms it. Moreover, our approach maintains strong performance even when number of jammers is four. For the remaining experiments, we compare our results only against the baseline, as it performs slightly better against jammers transmitting LoRa packets.

7.2.2 Varying Average Distance Between Jammers and Gateway. In this setup, we vary the average distance between three jammers and the gateway from 50 meters to 250 meters.



(a) Packet Reception Rate (b) Energy Per Packet

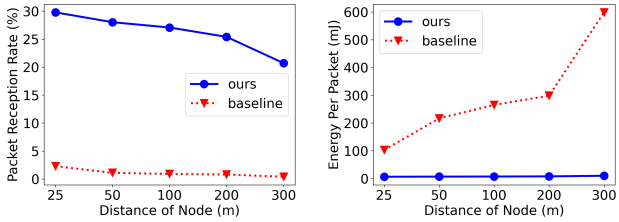
Figure 8: Performance varying average distance of jammers.

As illustrated in Figure 8(a), the PRR is higher for our approach when the jammers are near the gateway. The PRR improves for baseline when the jammers are moved away from the gateway. However, our approach achieves a PRR of 22.18%, while baseline achieves only 2.7% PRR when the jammer is at a 50-meter distance from the gateway, indicating an improvement of 8.21 times. For severe jamming conditions when the jammer is at a 50-meter distance, the improvement is 76.75 times. The PRR of our approach slightly decreases as the jammers are moved away from the gateway.

As shown in Figure 8(b), the EPP of our approach improves (decreases in value) as the jammers are moved near the gateway. The EPP improves for baseline when the jammers are moved away from the gateway. Our approach has an EPP of 9.32 mJ, while baseline incurs a very high EPP of 87.39 mJ when the jammer is at a 250-meter distance from the gateway, indicating an improvement of around 9.38 times. For severe jamming conditions when the jammer is at a 50-meter distance, the improvement is 94.74 times. The EPP of baseline decreases as the jammer is moved away from the gateway.

The PRR and EPP improvement with the jammer being near is attributed to the jammer's distinct energy peak in FFT bins. When the jammers are near the gateway, the probability of detecting and isolating the jamming energy peaks is higher.

7.2.3 Varying Distance Between Node and Gateway. In this setup, we vary the distance between the LoRa node and the gateway from 25 to 300 meters. As depicted in Figure 9(a), the PRR declines for



(a) Packet Reception Rate (b) Energy Per Packet

Figure 9: Performance varying distance of node.

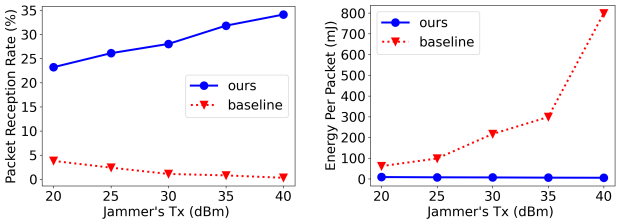
both our approach and baseline when the LoRa node is moved away from the gateway.

Our approach reaches a PRR of 29.78%, while baseline achieves only 2.38% PRR when the LoRa node is at a 25-meter distance from the gateway, indicating an improvement of 12.51 times. For worse conditions when the LoRa node is at a 300-meter distance, the improvement is 51.75 times. The PRR of our approach decreases slightly as the LoRa node is moved away from the gateway.

As shown in Figure 9(b), the EPP of our approach and baseline increases in value when the LoRa node is moved away from the gateway. our approach has an EPP of 6.56 mJ, while baseline incurs a very high EPP of 99.34 mJ when the LoRa node is at a 25-meter distance from the gateway, indicating an improvement of around 15.15 times. For worse conditions when the LoRa node is at a 300-meter distance, the improvement is 59.29 times. The EPP of our approach increases slightly as the LoRa node is moved away from the gateway.

The slight deterioration in PRR and EPP with the LoRa node being far away is caused by the slightly decreased probability of legitimate LoRa symbols having distinct peak in the FFT bins.

7.2.4 Varying Transmission Power of Jammers. For this setup, we vary the transmission power of the jammer from 20 dBm to 40 dBm, using 10 dBm transmission power at the LoRa node.



(a) Packet Reception Rate (b) Energy Per Packet

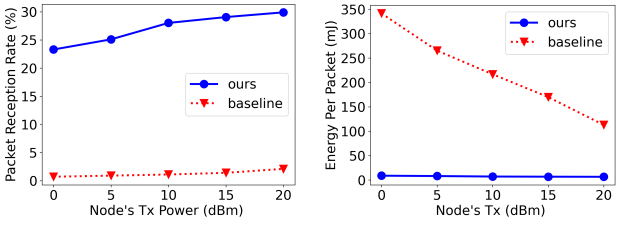
Figure 10: Performance varying transmission power of jammers.

As depicted in Figure 10(a), the PRR is higher for our approach when the transmission power of the jammers are increased. The PRR improves for baseline when the jammers have lower transmsision power. Our approach has a PRR of 34.14%, while baseline achieves only 0.32% PRR when the jammers' transmission power are 40 dBm, indicating an improvement of 106.56 times. When the jammers' transmission power are 20 dBm, the improvement is 6.11 times.

As shown in Figure 10(b), the EPP of our approach improves (decreases in value) when the transmission power of the jammers are increased. The EPP improves for baseline when the jammers have lower transmsision power. Our approach has an EPP of 5.54 mJ, while baseline incurs a very high EPP of 748.5 mJ when the jammer's transmission power is 40 dBm, indicating an improvement of 135.15 times. When the jammer's transmission power is 20 dBm, the improvement is 6.97 times.

The PRR and EPP improvement with the increasing jammers' transmission power is attributed to the jammer's distinct energy peak in FFT bins. When the jammers' transmission power is higher, the probability of detecting and isolating the jamming energy peaks improves.

7.2.5 Varying Transmission Power of Node. For this setup, we vary the transmission power of the LoRa node from 0 dBm to 20 dBm, using 30 dBm transmission power at the jammer.

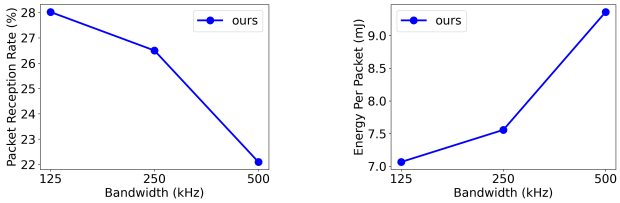


(a) Packet Reception Rate (b) Energy Per Packet

Figure 11: Performance varying transmission power of node.

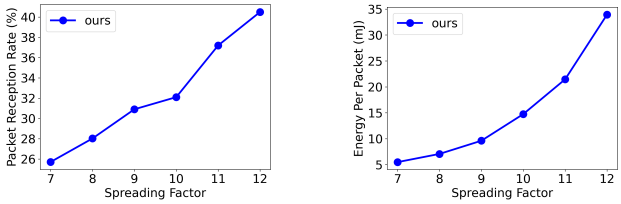
As depicted in Figure 11(a), the PRR increases for both our approach and baseline as the transmission power of the LoRa node is increased. our approach reaches a PRR of 29.97%, while baseline achieves only 2.17% PRR when the LoRa node's transmission power is 20 dBm, indicating an improvement of 13.8 times. Under worse conditions- when the LoRa node's transmission power is 0 dBm, the improvement is 33.29 times.

As shown in Figure 11(b), the EPP of our approach and baseline improves (decreases in value) as the transmission power of the LoRa node increases. our approach has an EPP of 6.51 mJ, while baseline incurs a high EPP of 109.1 mJ when the LoRa node's transmission power is 20 dBm, indicating an improvement of 16.76 times. When the LoRa node's transmission power is 0 dBm, the improvement is 38.79 times.



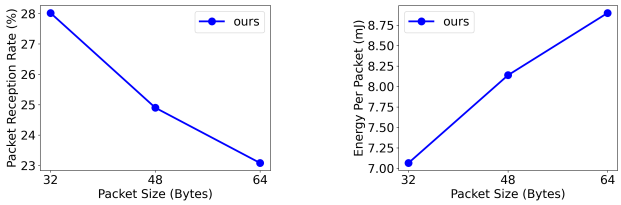
(a) Packet Reception Rate (b) Energy Per Packet

Figure 12: Performance varying bandwidth.



(a) Packet Reception Rate (b) Energy Per Packet

Figure 13: Performance varying SFs.



(a) Packet Reception Rate (b) Energy Per Packet

Figure 14: Performance varying packet size.

The PRR and EPP improve with the increasing LoRa node's transmission power. This occurs due to higher probability of detecting the legitimate LoRa symbol's peak in FFT bins, which results in better decoding of LoRa packet.

7.2.6 Varying Communication Parameters. We vary the bandwidth, spreading factor, and packet size in this setup. As illustrated in Figure 12, lower bandwidth performs slightly better. As depicted in Figure 13, the system achieves a higher PRR with a higher SF, though this incurs a higher energy cost due to longer packet air time. From Figure 14, it is evident that even with a larger packet size, performance is consistent.

7.3 Implementation Overhead and Real-time Feasibility

A critical consideration for any gateway-side solution is the computational overhead and its impact on real-time processing. Although our approach processes multiple signals in parallel, the underlying computations are simple and do not introduce significant latency. In our experimental implementation on a USRP-based gateway, we measured the additional processing time required by our technique compared to a standard LoRa decoder. For an entire 32-byte packet, our method adds an average overhead of approximately **3 ms**. This overhead is negligible when compared to the typical on-air time of a single LoRa symbol, which is often over 50 ms, depending on

the spreading factor. This demonstrates that our system is computationally efficient and fully capable of real-time operation on commodity hardware without compromising the gateway's ability to handle network traffic.

8 Conclusion

Jamming poses a significant threat to low-power wide-area network (LPWAN) communications due to their reliance on centralized gateways. In this paper, we have addressed the vulnerability of LPWAN, specifically LoRa, to wireless jamming attacks by proposing a new anti-jamming method. It entails implicit synchronization of all the LoRa symbols from different LoRa packets to ensure the jammers' energy in FFT bin remain distinguishable. This method is link layer-agnostic, entails no overhead at the LoRa nodes, and enables packet decoding even when facing attacks from a single jammer or multiple jammers on a channel. We have implemented and evaluated our anti-jamming system using COTS LoRa devices in outdoor experiments. Results demonstrate significant improvements in packet reception rates and energy efficiency compared to conventional LoRaWAN protocols, achieving up to 106.56 times enhancement in packet reception rate and reducing energy consumption per packet by up to 135.15 times. These findings demonstrates the effectiveness and practicality of our proposed anti-jamming technique in safeguarding LoRa networks against impending jamming threats, thereby enhancing the reliability and resilience of LPWAN communications.

ACKNOWLEDGEMENT

The work was supported by the US National Science Foundation through grants CNS-2301757, CAREER- 2306486, CNS-2306745, and by the US Office of Naval Research through grant N00014-23-1-2151.

References

[1] https://spectrum.ieee.org/satellite-jamming.
[2] https://www.i-scoop.eu/internet-of-things-guide/iot-network-lora-lorawan/.
[3] https://www.thethingsindustries.com/news/the-things-industries-expands-lorawan-network-capacity-by-supporting-lr-fhss-data-rates/.
[4] Arduino Uno Rev3. https://store-usa.arduino.cc/products/arduino-uno-rev3.
[5] Dragino gps/lora shield. https://www.dragino.com/products/lora/item/102-lora-shield.html.
[6] Ettus Research. https://www.ettus.com/product/.
[7] GNU Radio. http://gnuradio.org.
[8] LoRaWAN. https://www.lora-alliance.org.
[9] Mexico Q1-2023 cargo theft report. https://over-haul.com/wp-content/uploads/2023/05/Mexico-Q1-2023-Cargo-Theft-Report.pdf.
[10] Aras, E., Small, N., Ramachandran, G. S., Delbruel, S., Joosen, W., and Hughes, D. Selective jamming of lorawan using commodity hardware. In *MobiQuitous* (2017), pp. 363–372.
[11] Bardyn, J. P., Melly, T., Seller, O., and Sornin, N. Iot: The era of lpwan is starting now. In *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference* (2016), pp. 25–30.
[12] Daidone, R., Dini, G., and Tiloca, M. A solution to the gts-based selective jamming attack on ieee 802.15.4 networks. *Wirel. Netw. 20*, 5 (July 2014), 1223–1235.
[13] Dongare, A., Narayanan, R., Gadre, A., Luong, A., Balanuta, A., Kumar, S., Iannucci, B., and Rowe, A. Charm: exploiting geographical diversity through coherent combining in low-power wide-area networks. In *IPSN* (2018), IEEE, pp. 60–71.
[14] d'Oro, S., Galluccio, L., Morabito, G., Palazzo, S., Chen, L., and Martignon, F. Defeating jamming with the power of silence: A game-theoretic analysis. *IEEE transactions on wireless communications 14*, 5 (2014), 2337–2352.
[15] Eletreby, R., Zhang, D., Kumar, S., and Yağan, O. Empowering low-power wide area networks in urban settings. In *SIGCOMM* (2017), pp. 309–321.
[16] Gollakota, S., and Katabi, D. Zigzag decoding: Combating hidden terminals in wireless networks. In *SIGCOMM* (2008), pp. 159–170.
[17] Gollakota, S., Perli, S. D., and Katabi, D. Interference alignment and cancellation. In *SIGCOMM* (2009), pp. 159–170.
[18] Grover, K., Lim, A., and Yang, Q. Jamming and anti–jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing 17*, 4 (2014), 197–215.
[19] Haque, M. A., and Saifullah, A. A game-theoretic approach for mitigating jamming attacks in lpwan. *EWSN* (2023).
[20] Haque, M. A., and Saifullah, A. Handling jamming attacks in a lora network. In *IoTDI* (2024), IEEE, pp. 146–157.
[21] Haque, M. A., Saifullah, A., and Zhang, H. Deep reinforcement learning based coexistence management in lpwan. In *INFOCOM* (2025), IEEE, pp. 1–10.
[22] Hou, N., Xia, X., and Zheng, Y. Jamming of LoRa PHY and countermeasure. In *INFOCOM* (2021), IEEE, pp. 1–10.
[23] Huang, C.-Y., Lin, C.-W., Cheng, R.-G., Yang, S. J., and Sheu, S.-T. Experimental evaluation of jamming threat in LoRaWAN. In *VTC2019-Spring* (2019), IEEE, pp. 1–6.
[24] Ismail, D., Rahman, M., Saifullah, A., and Madria, S. Rnr: Reverse & replace decoding for collision recovery in wireless sensor networks. In *SECON* (2017), IEEE, pp. 1–9.
[25] Jain, A., Haque, M. A., Saifullah, A., and Zhang, H. Burst-mac: A mac protocol for handling burst traffic in lora network. In *RTSS* (2024), IEEE, pp. 148–160.
[26] Jain, M., Choi, J. I., Kim, T., Bharadia, D., Seth, S., Srinivasan, K., Levis, P., Katti, S., and Sinha, P. Practical, real-time, full duplex wireless. In *MobiCom* (2011), pp. 301–312.
[27] Katti, S., Gollakota, S., and Katabi, D. Embracing wireless interference: Analog network coding. *SIGCOMM 37*, 4 (2007), 397–408.
[28] Katti, S., Rahul, H., Hu, W., Katabi, D., Médard, M., and Crowcroft, J. Xors in the air: Practical wireless network coding. In *SIGCOMM* (2006), pp. 243–254.
[29] Kong, L., and Liu, X. mzig: Enabling multi-packet reception in zigbee. In *MobiCom* (2015), pp. 552–565.
[30] Lazos, L., Liu, S., and Krunz, M. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In *WiSec*.
[31] Li, C., Guo, H., Tong, S., Zeng, X., Cao, Z., Zhang, M., Yan, Q., Xiao, L., Wang, J., and Liu, Y. Nelora: Towards ultra-low snr lora communication with neural-enhanced demodulation. In *SenSys* (2021), pp. 56–68.
[32] Mikhaylov, K., Fujdiak, R., Pouttu, A., Miroslav, V., Malina, L., and Mlynek, P. Energy attack in lorawan: Experimental validation. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (2019), pp. 1–6.
[33] Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., and Pantziou, G. A survey on jamming attacks and countermeasures in wsns. *IEEE Communications Surveys Tutorials 11*, 4 (2009), 42–56.
[34] Pelechrinis, K., Iliofotou, M., and Krishnamurthy, S. V. Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications surveys & tutorials 13*, 2 (2010), 245–257.
[35] Pelechrinis, K., Koufogiannakis, C., and Krishnamurthy, S. V. Gaming the jammer: Is frequency hopping effective? In *2009 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks* (2009), pp. 1–10.
[36] Pirayesh, H., and Zeng, H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE communications surveys & tutorials 24*, 2 (2022), 767–809.
[37] Proano, A., and Lazos, L. Packet-hiding methods for preventing selective jamming attacks. *IEEE Transactions on Dependable and Secure Computing 9*, 1 (2012), 101–114.
[38] Raymond, D. R., and Midkiff, S. F. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing 7*, 1 (2008), 74–81.
[39] Saifullah, A., Rahman, M., Ismail, D., Lu, C., Liu, J., and Chandra, R. Low-power wide-area network over white spaces. *IEEE/ACM Transactions on Networking 26*, 4 (Aug 2018), 1893–1906.
[40] Statista. Number of Internet of Things (IoT) connected devices. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, 2021.
[41] Tong, S., Xu, Z., and Wang, J. Colora: Enabling multi-packet reception in lora. In *INFOCOM* (2020), IEEE, pp. 2303–2311.
[42] Wang, X., Kong, L., He, L., and Chen, G. mlora: A multi-packet reception protocol in lora networks. In *ICNP* (2019), IEEE, pp. 1–11.
[43] Wood, A. D., Stankovic, J. A., and Zhou, G. Deejam: Defeating energy-efficient jamming in ieee 802.15. 4-based wireless networks. In *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* (2007), IEEE, pp. 60–69.
[44] Xia, X., Chen, Q., Hou, N., Zheng, Y., and Li, M. Xcopy: Boosting weak links for reliable lora communication. *MobiCom* (2023).
[45] Xia, X., Zheng, Y., and Gu, T. Ftrack: Parallel decoding for lora transmissions. In *SenSys* (2019), pp. 192–204.
[46] Yang, D., Xue, G., Zhang, J., Richa, A., and Fang, X. Coping with a smart jammer in wireless networks: A Stackelberg game approach. *IEEE Transactions on Wireless Communications 12*, 8 (2013), 4038–4047.
[47] Yu, S., Xia, X., Zhang, Z., Hou, N., and Zheng, Y. Fdlora: Tackling downlink-uplink asymmetry with full-duplex lora gateways. In *SenSys* (2024), pp. 281–294.