



De-spreading Over the Air: Long-Range CTC for Diverse Receivers with LoRa

Shuai Tong, Yangliang He, Yunhao Liu, Jiliang Wang

Tsinghua University, Beijing, P.R. China

{tl19, heyl18}@mails.tsinghua.edu.cn, {yunhao, jiliangwang}@tsinghua.edu.cn

ABSTRACT

Unlicensed LPWANs on ISM bands share the spectrum with various wireless techniques, such as Wi-Fi, Bluetooth, and ZigBee. The explosion of IoT deployments calls for an increasing need for long-range cross-technology communication (CTC) between LPWANs and other techniques. Yet, existing technologies cannot achieve real long-range CTC for commodity wireless. We propose L2X, which provides long-range CTC to diverse receivers with LoRa transmitters. At the heart of L2X, we design an energy-concentrating demodulation mechanism that de-spreads LoRa chirps over the air. Therefore, L2X enables non-LoRa receivers to detect and demodulate LoRa signals even under extremely low SNR. We address practical challenges in L2X design. We propose a packet detection method to detect low-SNR LoRa transmissions at non-LoRa receivers. To decode LoRa transmissions, we accurately synchronize the demodulation window with incoming packets and propose a cross-domain demodulation approach to enhance the demodulation SNR. We implement L2X, all using commodity devices, and extensively evaluate its performance. The results show that L2X achieves 1.2 km CTC with the signal -9 dB below the noise floor, improving the distance by $30\times$ compared with state-of-the-arts.

CCS CONCEPTS

- Networks → Network protocol design.

KEYWORDS

Internet of Things, LPWAN, LoRa, CTC

ACM Reference Format:

Shuai Tong, Yangliang He, Yunhao Liu, Jiliang Wang. 2022. De-spreading Over the Air: Long-Range CTC for Diverse Receivers with LoRa. In *The 28th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '22), October 17–21, 2022, Sydney, NSW, Australia*. ACM, New York, NY, USA, 13 pages. <https://doi.org/10.1145/3495243.3560524>

1 INTRODUCTION

The past decade has witnessed an unprecedented proliferation of wireless technologies (e.g., Wi-Fi, Bluetooth, ZigBee, and LoRa) for connecting ubiquitous devices for Internet of Things (IoT). The deployment of all kinds of wireless devices is anticipated to grow as large as 75 billion by 2025 [1]. Popular wireless techniques contain



This work is licensed under a Creative Commons Attribution International 4.0 License.

ACM MobiCom '22, October 17–21, 2022, Sydney, NSW, Australia

© 2022 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-9181-8/22/10.

<https://doi.org/10.1145/3495243.3560524>

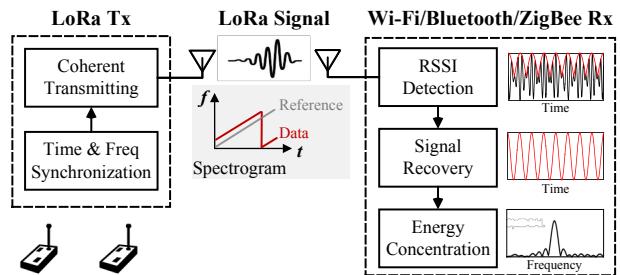


Figure 1: Illustration of L2X’s working principle.

two categories based on their communication ranges. The short-range wireless protocols (e.g., Wi-Fi, Bluetooth, and ZigBee) have a high data rate but are deficient in coverage. On the contrary, the long-range wireless protocols, e.g., LoRa, have a large coverage but are limited in the data rate. By pushing the information from the long-range wireless to short-range devices, we can bridge the technology gap, build more efficient IoT systems, and even enable applications that are previously impossible. For example, we can apply L2X for providing assistant links to isolated LoRa nodes that cannot connect to any of gateways, where the Wi-Fi/ZigBee/Bluetooth nodes can help to forward the LoRa information to the application servers. This is useful for developing regions without wireless infrastructure for long-range communication. L2X can also be used to share the channel information (e.g., channel frequency and active time) among heterogeneous networks to negotiate the channel settings on ISM bands. In this paper, we ask the question—“*Can we push the information from the long-range wireless (e.g., LoRa) to other wireless (e.g., Wi-Fi, Bluetooth, and ZigBee) directly for existing devices?*”

Existing Approaches. Much research effort has been made on CTC among short-range wireless protocols [2–12]. FreeBee [2] and WiZig [3] enable Wi-Fi to ZigBee CTC via Packet Probe Modulation (PPM). They encode data bits at Wi-Fi transmitters by adjusting the transmitting time and power of Wi-Fi packets. Then, ZigBee receivers decode incoming Wi-Fi packets through channel detection. PPM-based CTC approaches [2–6] have a low data rate of tens of bits per second, as they use each whole packet for encoding only several bits. Recent literature introduces high data-rate CTC via PHY-layer signal emulation [7–13]. For example, WeBee [7] and BlueFi [8] leverage Wi-Fi transmitters to emulate ZigBee and Bluetooth compliant packets by manipulating the payloads of Wi-Fi packets. Recently, LoRaBee [14] and XFi [15] try to push LoRa packets to short-range wireless via RSSI and CSI tracking.

Fundamental Limitations: The PHY-layer signal emulation demands high-end transmitters, which is not supported by the commodity low-cost LoRa. Meanwhile, the signal emulation often introduces SNR loss for the emulated signal [12], which is prohibited

for long-range CTC. Existing LoRa based CTC techniques (e.g., LoRaBee and XFi) do not leverage the properties of LoRa chirp signals and thus cannot achieve long-range communication. The key for LoRa long-range communication is to de-spread LoRa chirps for energy concentration on demodulation. However, existing CTC techniques cannot support chirp de-spreading at the non-LoRa receiver (e.g., Wi-Fi, Bluetooth, and ZigBee devices).

Our Approach. This paper proposes L2X, the first long-range CTC from LoRa to diverse wireless techniques (e.g., WiFi, Bluetooth, and ZigBee) with a communication range in the order of kilometers. L2X takes the benefit of LoRa chirp spreading spectrum modulation that enables chirp de-spreading and energy concentration at non-LoRa receivers based on RSSI sampling. Thus, it achieves high noise resistance for long-range CTC at diverse receivers. The simple requirements of L2X allow it to run on most commodity devices, which promises a low deployment cost for existing IoT systems.

The principle of L2X is shown in Figure 1. At the heart of L2X is an energy-concentrating demodulation mechanism that de-spreads LoRa chirps over the air. L2X adopts two collaborative LoRa devices at the transmitter side: one for transmitting data packets and the other for transmitting reference packets, e.g., standard LoRa beacons. By synchronizing those two transmitters both in time and frequency, the chirps from them are superposed and aligned in time over the same channel. While propagating over the air, we show that the superposed data chirp and reference chirp lead to signals with time-varying amplitudes. We theoretically prove that the frequency of this time-varying amplitude is the same as the de-spreading result of the data chirp. Thus, we can decode data chirps by analyzing the amplitude samples of the superposed signal at non-LoRa receivers. The decoding process, which is similar to de-spreading, can concentrate the energy in the data chirp, which leads to high noise resistance and long communication range.

Design Challenges. To realize the idea of L2X, we incorporate several novel designs to address practical challenges. (1) How to accurately detect low-SNR LoRa signal at non-LoRa devices? The signal can be drowned *below* the noise due to the long-range propagation and attenuation. Existing works fail to detect those low-SNR packets and thus cannot achieve long-range communication. We leverage the structure of the LoRa preamble for LoRa signal detection. We first divide the received signal into consecutive detection windows and then detect the LoRa packet by finding the pattern of consecutive energy peaks that correspond to repeated chirps in the preamble. (2) How to achieve time and frequency synchronization at both the transmitter side and the receiver side? We need synchronize the time and frequency between the L2X data and reference transmitters. Besides, we should align the demodulation windows at each L2X receiver with incoming LoRa packets. The unavoidable hardware imperfections (e.g., hardware delays and carrier frequency offsets) and the extremely low SNR of LoRa signals make the synchronization challenging. For the transmitter side synchronization, we first analyze the source of time and frequency offsets at LoRa hardwares and then compensate for the offsets at each transmitter. For the receiver side synchronization, we exploit the correlation with the conjugated chirps in the preamble for aligning demodulation windows with incoming LoRa packets. (3) How to demodulate the real low-SNR LoRa signal? The key for this challenge

is to aggregate energy of each chirp for demodulation. Theoretically, we can aggregate energy from the de-spreaded chirps by FFT with RSSI samples. In practice, we show that each de-spreaded chirp has two segments of different frequencies due to the cyclical frequency shift of LoRa payload chirps. Thus, the energy of those two segments cannot be aggregated for efficient demodulation. We propose a cross-domain demodulation approach that concentrates the energy of both segments by applying sampling interval control and spectrum merging.

We implement L2X on the commercial-off-the-shelf (COTS) devices and conduct extensive experiments to evaluate the performance. The results show that L2X can provide long-range CTC between LoRa and other wireless. Our main results and contributions are summarized as follows.

- To the best of our knowledge, L2X is the first end-to-end protocol that runs on top of COTS LoRa devices providing reliable long-range CTC to diverse non-LoRa receivers. It breaks the SNR boundary of existing CTC for reliable long-range connections with high noise resilience.
- To address practical challenges, we propose a LoRa packet detection approach to detect low-SNR signals even below the noise. We remove time and frequency offsets in signal transmissions by synchronizing the two transmitters. At the receiver, we achieve accurate window alignment and maximize the demodulation SNR for decoding by a cross-domain demodulation strategy.
- We implement L2X and evaluate its performance using COTS LoRa transmitters and diverse receivers, including ZigBee, Bluetooth, and Wi-Fi devices. The results show that L2X can achieve 1.2 km long-distance CTC to diverse receivers with the receiving signal -9 dB below the noise floor, improving the distance by $30\times$ compared with the state-of-the-art LoRaBee method.

2 BACKGROUND & MOTIVATION

LoRa Modulation and Demodulation. LoRa uses the Chirp Spreading Spectrum (CSS) at the physical layer for modulating signals into chirps of linear-varying frequencies [16]. LoRa chirps are inherently robust against noise, multi-path degradations, and Doppler effects. Thus, they can be detected and decoded under extremely low SNRs [17, 18]. The receiving sensitivity of a typical LoRa client is as low as -148 dBm, around 50 dBm lower than that of the Bluetooth [19, 20].

Fig 2(a) shows a base up-chirp with frequency increasing linearly throughout the whole bandwidth. LoRa encodes data bits into symbols by cyclically shifting the frequency of the base up-chirp. The LoRa chirp modulation incorporates two key parameters, i.e., spreading factor (SF) and bandwidth. SF determines the number of data bits that a LoRa chirp can modulate. For encoding SF bits with a single chirp, LoRa defines 2^{SF} different shifting frequencies. The frequency of an encoded LoRa chirp should be within the bandwidth BW , where signals with frequency higher than BW will align down to the lowest frequency, as shown in Fig 2(b). A LoRa receiver demodulates encoded up-chirps in two steps. First, it de-spreads the received chirp by multiplying it with a base down-chirp. The down-chirp is the conjugate of the base up-chirp; therefore, the de-spreading leads to a single tone with a frequency equal to the initial frequency of the received chirp. Then, the receiver applies

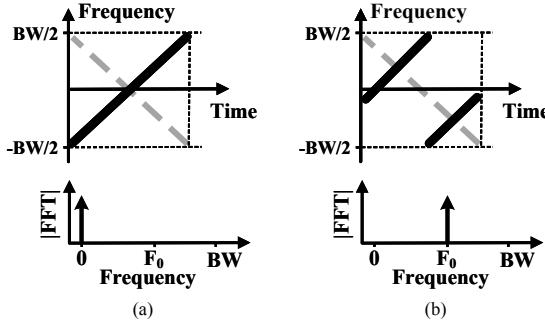


Figure 2: LoRa physical layer modulation mechanism with chirp spread spectrum.

FFT on the de-spreading signal, and decode the data by finding the associated FFT bin of the energy peak, as shown in Fig. 2.

CTC with LoRa. LoRa provides long-range and low-power wireless communication over the Sub-1 GHz and 2.4 GHz ISM bands. The bands of LoRa overlap with the operating frequency of many short-range wireless networks (e.g., Wi-Fi, Bluetooth, and ZigBee). Direct communication between LoRa and short-range wireless enables many IoT applications that are previously difficult to build. For example, by adding LoRa onto wireless mesh networks, we can efficiently reduce the overhead for network management as the key messages can be transmitted to sensors through direct long-distance links [21, 22]. Moreover, L2X also avoids cross-technology interference (CTI) problems, e.g., channel competition, signal collision, and throughput degradation, by channel occupancy negotiation among heterogeneous devices of different standards. This is meaningful for LoRa deployments especially considering the complex wireless coexistence situations in the wide coverage area of LoRa.

3 DE-SPREADING OVER THE AIR

In this section, we show how L2X de-spreads LoRa chirps over the air. Native LoRa receivers de-spread incoming signals by transforming the chirp's time-varying frequency to a single tone. Non-LoRa receivers do not support the chirp de-spreading operation, and thus they cannot decode LoRa packets for long-range CTC.

The key idea of L2X is to offload LoRa chirp de-spreading from the receiver to the signal propagation phase, i.e., de-spreading LoRa chirps by signal superposition over the air. When two LoRa chirps overlap over the air, the superposed signal has a periodical varying amplitude whose frequency is the same as the frequency difference between those two chirps. This indicates that we can obtain chirp de-spreading by creating signal superposition and then analyzing the amplitude of the superposed signal.

We show the mathematic model of our over-the-air chirp de-spreading. A LoRa chirp with the initial frequency of f_i is

$$C_i(t) = \alpha_i \cos[2\pi(f_i + kt/2)t + \varphi_i] \quad (1)$$

where φ_i is the initial phase of the chirp, and k is the slope of the frequency change. We use the time-varying angular frequency, i.e., $\omega_i = 2\pi(f_i + kt/2)$, for the sake of formula simplification. The superposition of two different LoRa chirps can be represented as

$$s(t) = \alpha_1 \cos(\omega_1 t + \varphi_1) + \alpha_2 \cos(\omega_2 t + \varphi_2) \quad (2)$$

To derive the amplitude pattern of the superposition, we transform the superposed signal to a more compact form. We first reconstruct

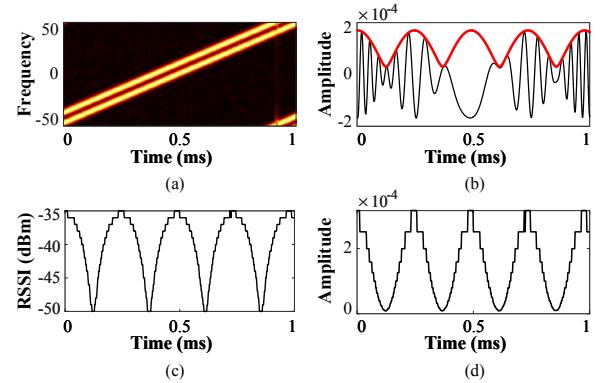


Figure 3: Illustration for chirp de-spreading over the air: (a) spectrogram and (b) time waveform for a chirp superposition, (c) RSSI trace at non-LoRa receivers, and (d) chirp de-spreading result from RSSI.

the phase expression of each chirp by applying the trigonometric formula. For example, we reconstruct the angular frequency of the chirp $C_1(t)$ as $\omega_1 = (\omega_1 + \omega_2)/2 + (\omega_1 - \omega_2)/2$. Therefore, the superposed chirp signal $s(t)$ can be expressed as

$$\begin{aligned} & \alpha_1 \cos \left[\left(\frac{\omega_1 + \omega_2}{2} t + \frac{\varphi_1 + \varphi_2}{2} \right) + \left(\frac{\omega_1 - \omega_2}{2} t + \frac{\varphi_1 - \varphi_2}{2} \right) \right] \\ & + \alpha_2 \cos \left[\left(\frac{\omega_1 + \omega_2}{2} t + \frac{\varphi_1 + \varphi_2}{2} \right) - \left(\frac{\omega_1 - \omega_2}{2} t + \frac{\varphi_1 - \varphi_2}{2} \right) \right] \end{aligned}$$

By $\cos(x+y) = \cos x \cdot \cos y - \sin x \cdot \sin y$ and merging similar items, we have

$$\begin{aligned} & (\alpha_1 + \alpha_2) \cos \left(\frac{\omega_1 - \omega_2}{2} t + \frac{\varphi_1 - \varphi_2}{2} \right) \cos \left(\frac{\omega_1 + \omega_2}{2} t + \frac{\varphi_1 + \varphi_2}{2} \right) \\ & - (\alpha_1 - \alpha_2) \sin \left(\frac{\omega_1 - \omega_2}{2} t + \frac{\varphi_1 - \varphi_2}{2} \right) \sin \left(\frac{\omega_1 + \omega_2}{2} t + \frac{\varphi_1 + \varphi_2}{2} \right) \end{aligned}$$

Finally, based on the auxiliary angle formula, we transform the above additive formula into a multiplicative one with the coefficient representing the amplitude. The obtained superposed signal is

$$s(t) = A \cos \left(\frac{\omega_1 + \omega_2}{2} t + \frac{\varphi_1 + \varphi_2}{2} + \Phi \right) \quad (3)$$

where A is the amplitude of the chirp superposition as

$$A = \sqrt{\alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2 \cos((\omega_1 - \omega_2)t + \varphi_1 - \varphi_2)} \quad (4)$$

and Φ is the instantaneous phase as

$$\Phi = \arctan \frac{(\alpha_1 + \alpha_2) \cos \left(\frac{\omega_1 - \omega_2}{2} t + \frac{\varphi_1 - \varphi_2}{2} \right)}{(\alpha_1 - \alpha_2) \sin \left(\frac{\omega_1 - \omega_2}{2} t + \frac{\varphi_1 - \varphi_2}{2} \right)} \quad (5)$$

We obtain the chirp de-spreading result of $C_1(t)$ from the signal amplitude in Eq. 4 as $\cos((\omega_1 - \omega_2)t + \varphi_1 - \varphi_2)$ when the frequency of the superposed signal $C_2(t)$ is known (i.e., ω_2 is known). L2X leverages this property for over-the-air chirp de-spreading by superposing the data chirp with a known reference chirp. Figure 3(a) and (b) show the time-frequency domain and time-amplitude domain waveforms of the chirp superposition. The chirp de-spreading result from the amplitude envelope is shown as the red curve in Figure 3(b). Note that the reference chirp is not necessarily a base up-chirp as long as its start frequency is known.

To decode LoRa packets at the non-LoRa receiver, we extract the signal envelope and recover the de-spreading result as shown in

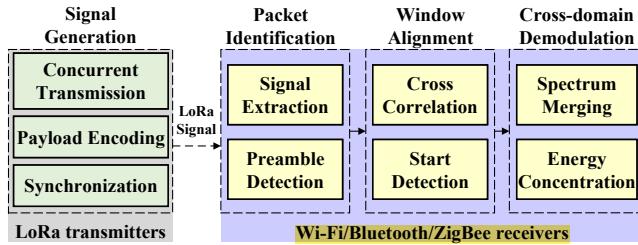


Figure 4: L2X’s architecture integrates LoRa signal generation (gray) and demodulation (purple).

Figure 3(c) and (d). We program Wi-Fi/Bluetooth/ZigBee devices to detect and decode LoRa packets during their carrier sensing operations, e.g., on the MAC-layer CSMA. The RSSI is inherently required by CSMA and is accessible from the corresponding registers. The receiver can obtain the RSSI and then detect the existence of a LoRa packet. At the same time, the receiver can detect the incoming native packet by detecting a receiving packet interrupt. The L2X packets will be corrupted upon concurrent native communication as the strength of native signals is much higher than that of LoRa signals. This promises the compatibility for L2X with normal operations of receivers as their native communications are not impacted.

To summarize, (1) the superposition of two LoRa chirps generates signals with time-varying amplitude whose envelope is the square root of the ideal chirp de-spreading result, and (2) other wireless devices can extract and decode the envelope signal from LoRa transmissions by sampling the RSSI over the wireless channel. The over-the-air chirp de-spreading brings the opportunity for enabling long-range CTC from LoRa transmitters to diverse wireless devices.

4 L2X OVERVIEW

L2X is a software solution that provides long-range CTC from LoRa to diverse IoTs (e.g., Wi-Fi, Bluetooth, and ZigBee). L2X exploits chirp de-spreading over the air to enable non-LoRa devices decode LoRa chirps by detecting the amplitude envelope of incoming signals. The de-spreading operation makes the CTC robust against channel attenuation and wireless interference.

The overall system design of L2X is as follows (see Figure 4). We use two LoRa nodes for the CTC transmission: one for sending the normal data and the other for transmitting a reference signal. Those two devices are synchronized both in time and frequency, so that they can concurrently transmit packets over the same channel. Note that the reference node can be a LoRa gateway that transmits mandatory LoRaWAN beacons as the reference signal. In such a case, the reference node does not introduce extra overhead. At the receiver, a Wi-Fi/Bluetooth/ZigBee device extracts the amplitude envelope of the incoming signal by RSSI sampling over the LoRa channel. It then recovers the chirp de-spreading results and identifies incoming LoRa packets from the RSSI samples. Finally, the receiver can successfully decode the LoRa packet by interpreting the demodulation results.

5 PACKET IDENTIFICATION

This section describes how L2X enables non-LoRa devices to identify incoming LoRa packets. For brevity, this section assumes that the

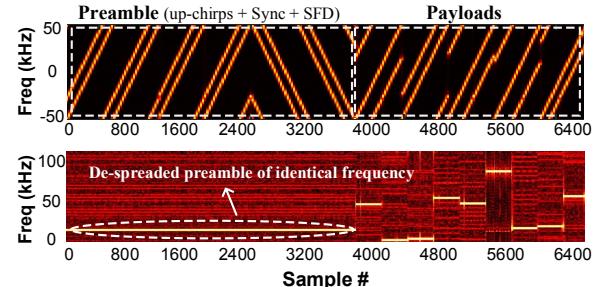


Figure 5: L2X’s packet identification by detecting LoRa preamble signals of the identical frequency.

two LoRa senders are synchronized. We will explicitly deal with synchronizing LoRa transmitters in Sec. 6.

- **Signal Extraction.** L2X explores using the amplitude envelope at non-LoRa receivers for detecting incoming LoRa packets. We extract the envelope signal by collecting RSSI samples with COTS devices, i.e., periodically reading values from the corresponding register. The RSSI is measured in decibels with reference to one milliwatt. Therefore, we extract the envelope signal by transferring RSSI to power values as $P(t) = 1mW \times 10^{RSSI/10}$. As is illustrated in Eq. 4, the power values $P(t)$ consists of the desired de-spreaded chirp signal and a DC component (i.e., $\alpha_1^2 + \alpha_2^2$ in Eq. 4). We finally remove this DC component from $P(t)$ with a digital DC isolation filter to obtain the desired de-spreaded chirp.

- **Preamble Detection.** After obtaining the de-spreaded chirp signal, we now explore how to identify low-SNR LoRa packets by detecting the incoming preamble. There are two challenges for preamble detection at non-LoRa receivers. First, signals from distant low-power transmitters may have extremely low SNRs. This is often overlooked in existing approaches. We should detect the preamble even when the signal is under the noise floor. Second, L2X should distinguish target transmissions from other wireless signals.

We propose an energy-enhanced packet detection approach leveraging the structure of the LoRa preamble. A typical LoRa preamble is composed of multiple consecutive base up-chirps. Assume a data packet has a frequency difference of f_0 with a reference packet. After de-spreading those two superposed packets, we should have consecutive preamble symbols with frequency f_0 . Based on this, we detect the low-SNR LoRa signal as follows: (1) We divide the signal into a series of consecutive detection windows. The length of each window is equal to the length of a chirp. (2) In each window, the superposed preamble chirps are de-spreaded to a single tone of frequency f_0 by envelope signal extraction. We concentrate the signal energy in each window by transforming preamble signals to FFT peaks in the frequency domain. The de-spreading and energy concentration also randomize the impact of channel noise. Thus, we can detect energy peaks for preamble chirps even under extremely low SNRs. (3) Finally, we detect the existence of the preamble by searching for identical FFT peaks in consecutive detection windows. In presence of interference, we identify the existence of a preamble when there are N_p consecutive windows each containing a peak within the frequency range of $(f_0 - \Delta f, f_0 + \Delta f)$, where N_p is the number of chirps in the preamble, and Δf is the tolerance for frequency estimation errors.

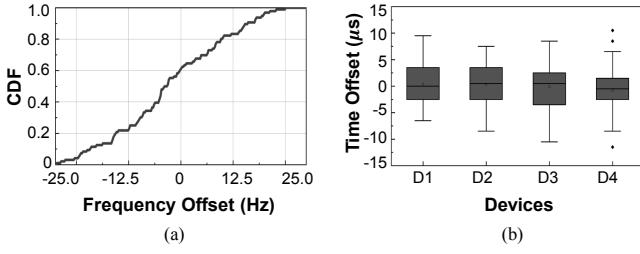


Figure 6: Accuracy for frequency and time synchronization for various LoRa transmitters.

6 SYNCHRONIZATION

6.1 Transmitter Side Synchronization

We first explore how to synchronize the data transmitter and reference transmitter in both time and frequency. To initialize the synchronization, the reference transmitter first acquires the medium and transmits a reference signal. Upon detecting the reference packet, the data transmitter switches to the transmitting mode and adjusts its local time and frequency. To achieve accurate synchronization, we address the following practical issues: (1) the hardware processing delays for transmitting and receiving signals, (2) different path propagation delays for signals from two transmitters to the receiver, and (3) Carrier Frequency Offsets (CFO) for local oscillators of two distributed transmitters.

To address those issues, we first evaluate the hardware processing delay for commodity devices. Our measurements show that the time for packet decoding, interrupt processing, and radio switching is nearly constant for a specific hardware platform. Therefore, we compensate the hardware processing delay by adjusting the packet transmitting time based on pre-estimations. We adjust the transmitting time of data packets with the granularity of micro-seconds which is the highest supported time accuracy for our STM32 based LoRa nodes. Then, we deal with the propagation delay that introduces a time offset between data and reference signals at the receiver. The time offset leads to decoding errors when it is larger than a basic time chip (i.e., $t_c = 1/BW$). We address this offset by taking the known frequency of LoRa preambles. When there is a time offset between the data and reference signals, de-spreaded signals of both pREAMbles and payloads are shifted by the same frequency. Thus, we estimate the preamble frequency and remove it from the payload de-spreading results for L2X payload demodulation. Finally, we estimate and compensate for the CFO. Commodity LoRa devices can measure the frequency offset between its local carrier and the incoming LoRa signal. The estimated value is a 20-bit integer in hertz stored in the Frequency Error Indicator (FEI) registers and can be addressed from the address of 0x28 to 0x2A for SX1276. Therefore, we cancel the CFO by extracting the value from the FEI registers and fine-tuning the carrier frequency of the data transmitter.

We evaluate the synchronization accuracy on four LoRa data transmitters of different vendors and radio chips. Device 1 and device 2 are with SX1276 and powered by battery and USB, respectively. Device 3 is with SX1268 and powered by a battery. Device 4 is with SX1280 and powered by USB. All of the four data transmitters are deployed closely to the reference transmitter to avoid the impact of propagation delays. Figure 6(a) shows the frequency

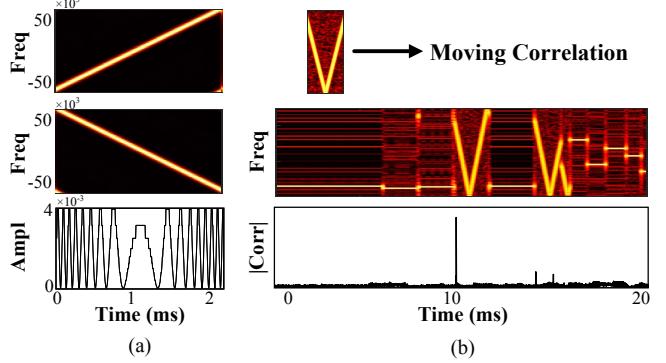


Figure 7: Receiver side synchronization: L2X aligns the demodulation window to the start of an incoming LoRa packet by detecting the peak from the correlation result.

of all transmissions are synchronized with an accuracy of $\pm 25\text{Hz}$. Figure 6(b) shows the time of the four data transmitters are synchronized with an accuracy of $10\mu\text{s}$. The residual synchronization errors and time offsets caused by propagation delays are further resolved in the payload decoding by taking the frequency of pREAMbles as a reference.

6.2 Receiver Side Synchronization

At the receiver, we need to align the demodulation window with the incoming packet. Our key idea is to determine the accurate packet start by exploiting the conjugated chirps (i.e., base up-chirps and down-chirps) in a LoRa packet. Recall the analysis in Sec. 3, the superposition of two chirps of the same type (e.g., two up-chirps) leads to the single-tone envelope signal for chirp de-spreading. However, the superposition of two chirps of different types (e.g., an up-chirp and a down-chirp) leads to the envelope signal with linearly varying frequencies, as shown in Figure 7(a). This brings opportunity for transferring small time misalignments to significant correlation coefficient changes by performing cross correlation with such a frequency-varying envelope signal. We leverage this observation for receiver synchronization.

We generate superposition of an up-chirp and a down-chirp by controlling the preamble length of the data packet. The number of base up-chirps in a LoRa preamble can be adjusted from 6 to 65535 [19]. In our implementation, we set the preamble of the data packet to have one more up-chirp than the reference packet. Therefore, the last up-chirp in the preamble of the data packet is superposed with the down-chirp (i.e., the Start Frame Delimiter, SFD) of the reference packet as shown in Figure 7(b). The superposition of those two conjugate chirps results in a *chirp* for the envelope signal, whose frequency varying rate is twice of the base up-chirp. We then use cross correlation to derive the start of the packet. Specifically, we use a locally generated reference chirp to correlate with the received envelope signal. There should be a clear correlation peak when the start of the generated reference is exactly aligned with the chirp in the envelope signal, as shown in Figure 7(b). Then, we detect the index of the correlation peak and derive the start of the received packet by subtract the known preamble length from the detected peak index. Based on the detected packet start, we can

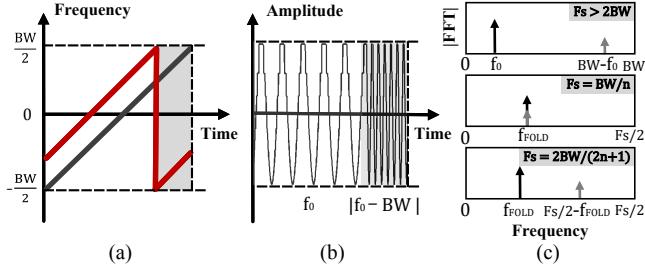


Figure 8: Cross-domain symbol demodulation based on spectrum merging.

finally determine the demodulation windows, each strictly aligned with a LoRa symbol.

7 CROSS-DOMAIN DEMODULATION

Till now, we have synchronized the demodulation window with the incoming packet. Then, we show how to decode data bits from low-SNR LoRa signals. The key idea is to aggregate the energy of the envelope signal by transforming it from the time domain to the frequency domain. After de-spreading over the air, the signal in each demodulation window is transformed to a single tone. Intuitively, we can apply FFT for signals in each window and find energy peaks in the frequency domain. Then, we obtain the demodulation data from the highest peak in the FFT result. However, this is not effective in practice due to the cyclical frequency shifting of LoRa payload modulation. As shown in Figure 8(a), part of the payload chirp with frequencies higher than $BW/2$ will be aligned down to the lowest frequency at $-BW/2$. This leads to two different frequencies in the chirp de-spreading result, i.e., the payload frequency shift f_0 and the wrapped frequency $|f_0 - BW|$, as shown in Figure 8(b). Thus, simply applying FFT on the signal leads to energy loss for peak detection, affecting chirp demodulation.

We propose a spectrum merging approach to address this problem for two cases. The first case is that the LoRa RSSI sampling rate is higher than twice the LoRa bandwidth. (1) We have two separated peaks for a LoRa payload chirp in the frequency domain. As shown in the top of Figure 8(c), those two FFT peaks are symmetric in the spectrum of $(0, BW)$, at f_0 and $BW - f_0$, respectively. (2) We flip the spectrum of $(0, BW)$ by moving the FFT result of the highest frequency to the lowest frequency. Thus, the peak at $BW - f_0$ in the original spectrum is now located at the frequency of f_0 . (3) We finally superpose the flipped spectrum with the original one to aggregate the energy of those two FFT peaks.

For effective spectrum merging, the two peaks for superposition should be in phase to avoid spectral leakage. However, the envelope signal in real values does not support phase compensation in the time and frequency domain. Therefore, before energy concentration, we apply Hilbert transform [23] to the envelop and construct a complex I/Q stream. The Hilbert transform is a linear system that imparts a phase shift of $\pi/2$ to every frequency component for the input signal. Thus, we use the original real values $S_I(t)$ and its Hilbert transform $S_Q(t)$ to synthesize the complex I/Q stream as $S(t) = S_I(t) + jS_Q(t)$. After constructing a complex stream from the original envelope, we leverage the adaptive phase compensation strategy in [24] for spectrum merging. We first transform the

synthesized $S(t)$ to the frequency domain as $\mathcal{F}\{S(t)\} = R(f)$ by FFT. Then, we adjust the phase of energy peaks by multiplying the flipped spectrum with $e^{j\Phi}$ before the spectrum superposition. We search for the optimal phase compensation via:

$$\Phi = \arg \max_{0 < \Phi \leq 2\pi} R_{(0, BW)}(f) + R_{(F_s - BW, F_s)}(f) \cdot e^{j\Phi} \quad (6)$$

The maximum can be obtained only when the phase difference between the two superposed peaks is perfectly compensated. The searching step is set in prior, e.g., 5 ~ 20 steps from 0 to 2π based on the signal quality. For high quality signal, we can even directly find the peak without searching. For each round of search, we perform the spectrum superposition with a computation complexity of $O(N)$. Therefore, the phase compensation has a low overall computation overhead and can be processed in real-time for our low-power IoT end nodes. Based on the phase searching result, we can finally concentrate the energy of the entire payload symbol and estimate its accurate frequency for demodulation.

The second case is that the sampling rate is less than twice of the LoRa bandwidth. We propose a sampling control strategy to concentrate the signal energy. Based on Nyquist sampling theorem, when the sampling rate $F_s < 2BW$, there will be spectrum aliasing where frequency $f_i > F_s/2$ are folded to the range of $(0, F_s/2)$ as

$$f_{FOLD} = \left| \text{mod}(f_i + \frac{F_s}{2}, F_s) - \frac{F_s}{2} \right| \quad (7)$$

Intuitively, if we set the sampling rate to an integer part of the BW , i.e., $F_s = BW/n$, $n = 1, 2, \dots$, the peaks of f_0 and $f_0 - BW$ will appear at the same location in the spectrum as shown in the middle of Figure 8(c). However, those two peaks may have different initial phases and thus direct spectrum folding can lead to severe spectral leakage. Thus, we set the sampling rate $F_s = 2BW/(2n+1)$. Thus, we have two peaks of different frequencies locating symmetrically in the spectrum, as shown in the bottom of Figure 8(c). Similar to spectrum merging of $F_s > 2BW$, we flip the spectrum, compensate the phase of those peaks, and then add those two peaks constructively. The energy of the payload signal can thus be effectively concentrated for demodulation. It is worth noting that the sampling control strategy of L2X does not break the Nyquist-Shannon sampling theorem. LoRa symbols with inadequate Nyquist sampling rate still cannot be recovered due to frequency aliasing. COTS LoRa (e.g., SX1276) supports a wide range of bandwidth from 7.8kHz to 500kHz. Thus, we can select an appropriate bandwidth for LoRa transmitters given a sampling rate at the receiver. Besides, even when the sampling rate is lower than the LoRa bandwidth, L2X can still work by adopting a payload manipulating scheme at the transmitter. For example, for the SF12 symbol, we use its eight least significant bits (LSB) for payload modulation and discard the 4 most significant bits (MSB). Thus, we can decode the data bits by detecting the aliased frequency.

8 ANALYSIS

We present an analysis on the receiving sensitivity of L2X and show that the de-spreading over the air introduces a very small SNR loss, allowing L2X to demodulate under very low SNRs.

L2X decodes LoRa packets by detecting the amplitude of superposed chirps (see Sec. 3). Denote $r(t) = s(t) + w(t)$ as the received signal for L2X's amplitude detection, where $s(t)$ is the superposed

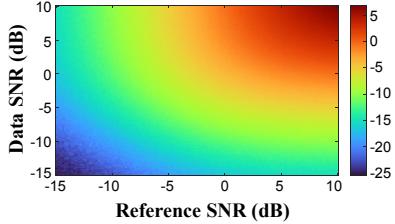


Figure 9: The SNR of de-spreading signal with data and reference packets under various SNRs.

SF	SNR Threshold	SF	SNR Threshold
7	-7.0dB	10	-11.0dB
8	-8.3dB	11	-12.4dB
9	-9.7dB	12	-13.7dB

Table 1: SNR thresholds of data and reference packets for L2X demodulation across SFs.

chirps with time-varying amplitude $A(t)$ as in Eq. 3, and $w(t)$ is the channel noise whose amplitude $n(t)$ follows the Gaussian distribution with a variance of σ^2 . The noise in the received signal is determined by the channel bandwidth of the receiver. As the channel bandwidth increases, a receiver listening on the bandwidth will pick up more in-band noise. The power of the noise can be represented as

$$N = k \times T(k) \times B(\text{Hz})$$

where k is Boltzmann's constant ($1.38E - 23J/K$), T is temperature on the Kelvin scale, and B is receiving bandwidth. The amplitude of the received signal can be represented as

$$|r(t)| = \sqrt{[A(t) + n(t)]^2} \quad (8)$$

L2X obtains the de-spreading result from the amplitude $|r(t)|$ by calculating its square. We substitute the complete form of $A(t)$ in Eq. 4 to $|r(t)|$ and calculate its square as

$$\begin{aligned} |r(t)|^2 &= \alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2 \cos((\omega_1 - \omega_2)t + \varphi_1 - \varphi_2) \\ &\quad + n^2(t) + 2n(t)\sqrt{\alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2 \cos \Phi(t)} \end{aligned} \quad (9)$$

α_1 and α_2 are the signal strength of the data packet and the reference packet, which is determined by the signal power spectrum density (PSD) E_{bi} and the signal bandwidth B_s as $\alpha_i^2 = E_{bi} \times B_s$. We remove the DC component of $\alpha_1^2 + \alpha_2^2$ by applying a DC isolation filter. The DC filter also removes the non-zero components from the noise. The rest of the $|r(t)|^2$ consists of the target de-spreading chirp signal

$$S_d(t) = 2\alpha_1\alpha_2 \cos((\omega_1 - \omega_2)t + \varphi_1 - \varphi_2) \quad (10)$$

and the zero-mean noise. We focus on the lowest SNR required for the L2X demodulation. Thus, we assume that both the data packet and the reference packet are received with a very low SNR, i.e., α_1 and α_2 are much smaller than the noise density (i.e., the noise power to 1Hz bandwidth, denoted as $N_0 = k \times T = \sigma^2/B$). The noise item with $\sqrt{\alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2 \cos \Phi(t)}$ is much smaller than $n^2(t)$ and can be neglected for estimating the SNR of the de-spreading signal. Thus, the main part of the noise is

$$n_d(t) = n^2(t) - E(n^2(t)) \quad (11)$$

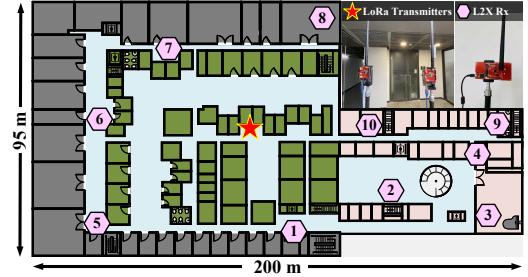


Figure 10: The indoor floor plan and devices spread out across tens of office rooms.

where $E(\cdot)$ is the mean operation. $n^2(t)$ is the square of a normal distribution whose variance is $\sigma^2 = N_0B$. Thus, $n^2(t)/\sigma^2$ follows the chi-square distribution with one degree of freedom and mean value 1. Based on this, we have $E(n^2(t)) = N_0B$ and the noise power for $n_d(t)$ in Eq. 11 is

$$\begin{aligned} P_n &= E(n^4(t) + \sigma^4 - 2\sigma^2 n^2(t)) \\ &= E(n^4(t)) - N_0^2 B^2 \end{aligned} \quad (12)$$

For a standard normally distributed variable, the mean of its fourth power equals to 3. Thus, we have $E(n^4(t)) = 3N_0^2 B^2$. The noise power in Eq. 12 is $P_n = 2N_0^2 B^2$. The signal power in Eq. 10 is $P_s = 4\alpha_1^2 \alpha_2^2 = 4E_{b1} B_s \times E_{b2} B_s$. Therefore, the SNR of $S_d(t)$ is

$$SNR_d = 10 \lg \frac{P_s}{P_n} = 3.01 + 10 \lg \frac{B_s^2}{B^2} + SNR_{data} + SNR_{ref} (\text{dB}) \quad (13)$$

where B_s/B is the ratio between the signal bandwidth and the noise bandwidth (i.e., receiving bandwidth), which is negative to the demodulation SNR when the noise bandwidth is wider than that of the signal. We first emulate the data packet and reference packet with different SNRs and calculate the SNR of de-spreading signals. Figure 9 shows the result. We can see that the SNR of the de-spreading signal decreases as decreasing of either the data SNR or the reference SNR. We further verified that the emulated SNR in Figure 9 is consistent with the theoretical analysis in Eq. 13. Based on the SNR threshold for standard LoRa chirp demodulation [25], we further derive the lowest SNR requirements of data and reference packets at different SFs with a bandwidth of 125kHz. We assume that both the data and reference packets are received at the same SNR. The results are shown in Table 1. Compared with the SNR threshold of native LoRa, L2X has a very small sensitivity loss, allowing it for reliable long-range CTC.

9 IMPLEMENTATION

Hardware and software. We implement L2X with commodity wireless transceivers. For packet transmission, we use commodity LoRa end nodes with SX1276 [19] and SX1280 [26] for sending signals at 915 MHz and 2.4 GHz, respectively. The LoRa nodes send LoRa signals at 24 dBm. At the receiver, we use Bluetooth, ZigBee, and Wi-Fi devices for demodulating and decoding LoRa signals. We achieve RSSI sampling by a function call for TI CC2652R (Bluetooth) and CC1310 (ZigBee) chips in our implementation. We achieve RSSI sampling on Wi-Fi devices with the CSITool software platform [27]. The RSSI values are either processed (i.e., de-modulated) on the

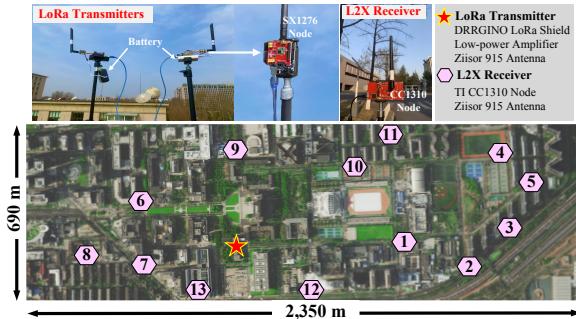


Figure 11: Bird view of the outdoor experiment field with LoRa transmitters and ZigBee receivers.

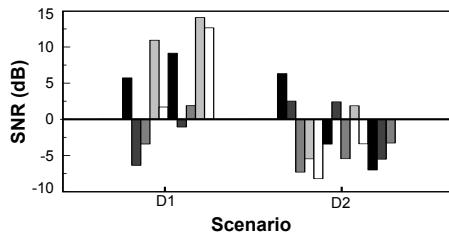


Figure 12: SNR Distribution for the deployments: D1 is the indoor deployment and D2 is the outdoor deployment.

node or flushed to a PC for analysis, depending on experiments. By default, the spreading factor (SF) and bandwidth (BW) of LoRa packets are set to 12 and 125kHz, respectively.

Experiment setups. We evaluate L2X's performance in both indoor and outdoor environments:

- **Indoor scenario.** As shown in Figure 10, we place LoRa transmitters and L2X receivers in a 200 m × 95 m office building. The rooms are separated by concrete walls. We deploy the transmitters in one office and move the receiver to over 10 different locations. The received SNR at the 10 locations was approximately -6~15dB, as shown in Figure 12. Due to the blockage of walls, most transmissions are under the non-line-of-sight (NLoS) condition, and the signal is severely attenuated. This scenario is representative of a realistic large scale indoor deployment.

- **Outdoor scenario.** We further deploy a campus-scale outdoor testbed. We place the transmitters on the roof of a four-story office building. We move the receiver to 13 different locations to collect LoRa packets in both LoS and NLoS conditions with various distance. The bird view of the outdoor testbed is shown in Figure 11. The received SNR significantly varies across the different receiving locations, ranging from -8 dB to 7 dB (see Figure 12). Most of the received signal in this deployment is below the noise floor and the signal fluctuates as pedestrians and traffic pass by.

Evaluation Metrics. We adopt four metrics to evaluate the performance of L2X: i) *Symbol Error Rate (SER)* measures the demodulation performance of L2X at the symbol level; ii) *Packet Delivery Ratio (PDR)* computes the packet reception rate, where a successful packet reception requires more than 80% of the symbols are correctly decoded; iii) *Throughput* is derived with the received packets, denoted as bits per second; iv) *Energy Consumption* computes the energy consumed for decoding each bit, denoted as mJ per bit.

Baselines. We compare L2X with two state-of-the-art (SoTA) CTC approaches for communication between LoRa and short-range wireless, i.e., packet probe modulation-based FreeBee [2] and energy trace-based LoRaBee [14]. We also adopt the standard ZigBee and native LoRa as baselines.

10 EVALUATION & RESULTS

In this section, we evaluate the performance of L2X to answer the following questions.

- **Q1 (§10.1)** How much does L2X improve the demodulation performance compared with state-of-the-art CTC techniques and standard short-range wireless?
- **Q2 (§10.2)** What is the energy efficiency of L2X for receiving LoRa packets at non-LoRa devices?
- **Q3 (§10.3)** How does L2X perform in various real-world deployments, including indoor/outdoor, low/high noise, and LoS/NLoS scenarios?
- **Q4 (§10.4)** How well does L2X perform with Wi-Fi and Bluetooth receivers?

10.1 Overall Comparisons with SoTAs

Setup: We evaluate the performance of L2X and SoTAs with the indoor testbed under various SNR settings and LoRa configurations, including three SFs (8, 10, 12) and three BWs (62.5 kHz, 125 kHz, 250 kHz). We deploy the LoRa transmitters and L2X receivers at the same room and adopt a USRP N210 [28] for transmitting white Gaussian noise over the LoRa channel. Thus, by adjusting the transmitting power of the USRP, we can generate LoRa packets with different SNRs. We implement the L2X receiver on a ZigBee node with the CC1310 [29] chip. The sampling rate of the node is 25 kHz. We compare L2X's SER and throughput with LoRaBee [14] under various LoRa SF and BW configurations. The PPM-based FreeBee [2] approach is not affected by LoRa SF and BW changes. Thus, we compare L2X with FreeBee and standard ZigBee in terms of the SNR threshold which is the minimum SNR requirement for decoding 80% of transmitted packets.

Results: We present the performance comparison of L2X and SoTAs for different LoRa SF and BW configurations.

- **Evaluation of SF configurations.** Figure 13(a) shows the SER performance of L2X and LoRaBee with different SFs and SNRs for BW 125 kHz. Both L2X and LoRaBee have performance improvements with higher SFs. This is because a higher SF leads to a longer chirp length. For LoRaBee, a longer chirp length makes it easier to detect the down edges of the LoRa energy trace. For L2X, a longer chirp length leads to more concentrated signal energy in demodulation. LoRaBee requires a chirp length no less than 8ms. Thus, we can only show the evaluation results of LoRaBee for SF 10 and 12. Figure 13(a) also shows that the SERs of both L2X and LoRaBee increase as the LoRa SNR decreases. LoRaBee decodes LoRa payloads by detecting energy trace of received signals. Thus, as the SNR decreases, the channel noise quickly overwhelms the time-domain energy trace, causing a rapid SER increase when the SNR is lower than 6 dB. In contrast, the SER of L2X increases much slower than LoRaBee, and the SER remains low even when the signal power is lower than the noise, i.e., SNR < 0. This is because L2X takes the benefit of chirp de-spreading for energy concentration. As a result,

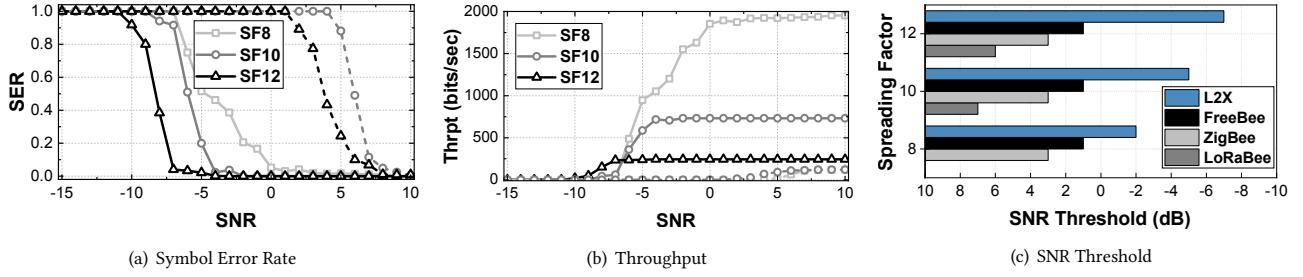


Figure 13: Performance comparison for L2X and SoTAs with different SF configurations and various SNRs: Solid lines in (a) and (b) indicate the performance of L2X and dashed lines correspond to LoRaBee.

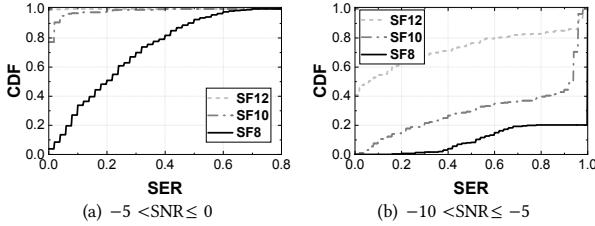


Figure 14: CDF of L2X's SERs with different SF.

L2X achieves high noise resistance and long-range transmissions even when signals are severely attenuated during propagation.

Figure 14(a) and 14(b) show the detailed SER performance of L2X with different SFs. When the SNR is $-5 \sim 0$ dB, almost 100% high-SF (10, 12) transmissions and 50% low-SF (8) transmissions have the SER < 0.2 as L2X can reduce the noise interference by cross-domain energy concentration. When the SNR < -5 dB, the successful packet delivery with SER < 0.2 for the three SFs are 1%, 16%, and 63%, respectively. In practice, small SFs in LoRa are used for near-area high data-rate transmissions. Thus, we can increase the SF for improving decoding performance in low-SNR scenarios.

Figure 13(b) shows the throughput of L2X and LoRaBee with various SF configurations. The throughputs of FreeBee and ZigBee are not compared as they are not impacted by the SF. LoRa packets with small SFs provide high data rates for both L2X and LoRaBee, as a smaller SF leads to shorter channel time for each chirp. For all SNRs, L2X has a much higher throughput than LoRaBee, as L2X encodes more bits in each chirp and experiences lower SERs. Figure 13(c) shows the SNR thresholds of L2X and three SoTAs. LoRaBee, FreeBee and native ZigBee decode packets based on time-domain characteristics such as signal phase and energy. Therefore, they all require the signal power higher than the noise, i.e., $\text{SNR} > 0$ dB. L2X benefits from chirp de-spreading and achieves an SNR threshold of -7 dB in SF12, which is much better than SoTAs.

• **Evaluation of BW configurations.** We demonstrate the impact of the signal bandwidth on L2X by estimating the SER and throughput under various SNRs with SF=12. The ZigBee and FreeBee transmissions are not impacted by the LoRa bandwidth configuration. Therefore, we compare them with L2X in terms of SNR thresholds in Figure 15(c). Figure 15(a) illustrates the SER of L2X and LoRaBee with three different BWs. As the BW decreases, the SER of L2X decreases due to the longer chirp duration and less in-band noise and interference. On the contrary, the SER of LoRaBee increases as the BW decreases. This is because the LoRaBee requires the ZigBee

TEST OPERATIONS	CURRENT
Active MCU	2.5 mA
MCU + Radio Tx	11.2~25.1 mA
MCU + Radio Rx	5.5 mA
Standby	0.7 μ A

Table 2: Estimation of current on a CC1310 based L2X receiver under various operations. The device is powered at 3.6V.

channel to overlap with the LoRa band for collecting RSSI traces. A narrow bandwidth leads to low energy tracking accuracy and thus a high SER. The SER of L2X outperforms LoRaBee with all three BWs under all SNR settings due to the benefit of chirp de-spreading and energy concentration. Figure 16(a) and Figure 16(b) show the CDF of L2X's SER with different BWs. When the SNR is $-5 \sim 0$ dB, most transmissions of 62.5 kHz and 125 kHz have SERs lower than 0.01; over 97.5% transmissions of 250 kHz have SERs < 0.2 . When the SNR < -5 dB, the median SER for 62.5 kHz, 125 kHz, and 250 kHz is 0, 0.06, and 0.26, respectively, demonstrating high link reliability.

Figure 15(b) shows the throughput of L2X and LoRaBee. As the bandwidth increases, both L2X and LoRaBee obtain throughput improvements as LoRa chirps with larger bandwidth have a much shorter channel time. For all BW settings, the throughput of L2X is much higher than that of LoRaBee, as L2X encodes more bits in each chirp than LoRaBee. The receiver sensitivity of L2X also outperforms LoRaBee, allowing L2X getting a much higher throughput especially for low-SNR situations. We finally compare the SNR threshold for L2X, FreeBee, LoRaBee, and native ZigBee in Figure 15(c). We can see that L2X outperforms all other methods by pushing the SNR threshold to -9 dB with a bandwidth of 62.5 kHz.

10.2 Energy Consumption

Setup: In this experiment, we measure the energy profile of L2X receivers. The measurements of energy consumption show the possibility for applying L2X in low-power IoT end devices. In the experiment, we first measure the current of a CC1310 [29] ZigBee receiver with a Monsoon HV Power Monitor [30] under different operations, including MCU computing, radio transmission, RSSI collection, and sleeping. Then, we estimate the receiver power consumption by multiplying the measured current with the input voltage (i.e., 3.6V in our experiment) and accumulating the multiplication result over time. Finally, we simulate the battery life of L2X receivers based on their energy consumption given the battery

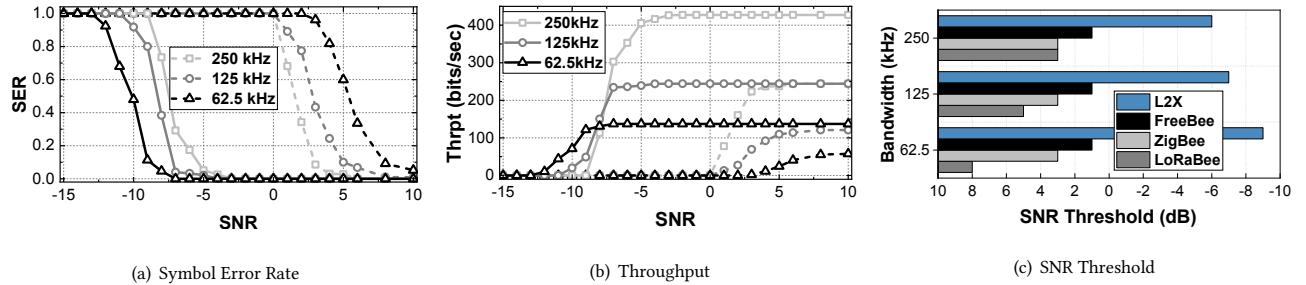


Figure 15: Performance comparison for L2X and SoTAs with different bandwidths and various SNRs: Solid lines in (a) and (b) indicate the performance of L2X and dashed lines correspond to LoRaBee.

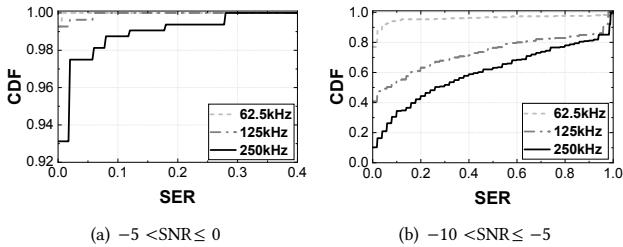


Figure 16: CDF of L2X's SERs with three different BW configurations at two SNR ranges.

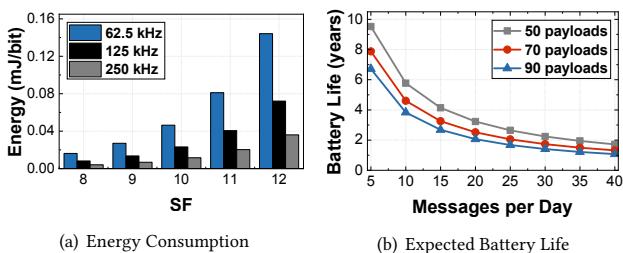


Figure 17: Energy consumption for ZigBee CC1310 based L2X receivers: (a) Energy cost, (b) Expected battery life under different duty cycles and packet lengths.

capacity of 2200 mAh. Note that we use LoRa devices with tethered power supplies as L2X transmitters, so we do not consider the energy consumption at the transmitter side.

Results: Table 2 shows the current profile of the CC1310 receiver. L2X decodes LoRa packets by continuously collecting RSSI in the radio Rx mode with a current consumption of 5.5mA. Compared with the native packet reception of ZigBee, L2X introduces very limited additional energy consumption for RSSI sampling. Thus, L2X does not introduce significant energy consumption compared with native techniques. Based on the current estimation, we derive the energy cost for receiving LoRa packets of 50 payload symbols with various SFs and bandwidths in Figure 17(a). We observe that the total energy consumption for L2X receivers is related to the SF and bandwidth, as a larger SF or narrower bandwidth leads to a longer packet and thus higher energy consumption. We further translate the energy cost to the battery life. We assume that a L2X receiver with a 700 mAh battery continuously receives LoRa packets with SF12 and 125kHz bandwidth. Figure 17(b) presents the battery life of the L2X receiver. With the longest packet length, the battery-powered L2X receiver can work for nearly two years

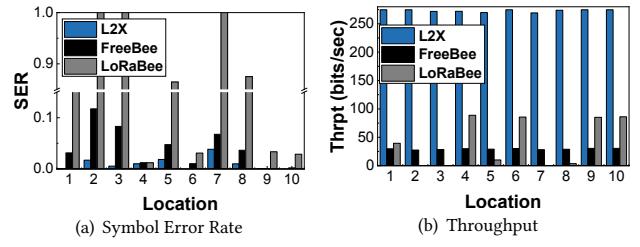


Figure 18: SER and Throughput of L2X at 10 locations of the indoor deployment.

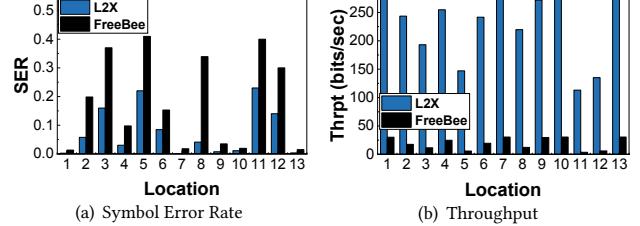


Figure 19: SER and Throughput of L2X at 13 locations of the outdoor campus-scale deployment.

for 40 transmissions per day. L2X receivers can further extend their battery life by lowering the rate for LoRa packet reception.

10.3 Real-World Deployments

Setup: We evaluate the performance of L2X in real-world deployments of both indoor and outdoor environments. For each deployment, we configure the LoRa transmitters to send LoRa packets in a duty cycle of 10% with SF 12 and bandwidth 125kHz. We move the L2X receiver to tens of indoor/outdoor locations to evaluate its performance in different environments. Besides, we evaluate the impact of the distance between data and reference transmitters on the L2X performance. We deploy the data and reference senders outdoors and change their distance from 0.3 to 1.8km. We deploy the receiver between the two senders and evaluate its PDR and throughput with different Tx distances.

Results: Figure 18 presents the SER and throughput of L2X and SoTAs at ten different indoor locations. L2X achieves the lowest SER and the highest throughput at all evaluated locations compared with SoTAs. LoRaBee decodes LoRa symbols by detecting changes in energy traces, and thus it requires a high receiving SNR and is vulnerable to interference. FreeBee leverages the signal time for decoding data bits, which is more reliable than LoRaBee but still has

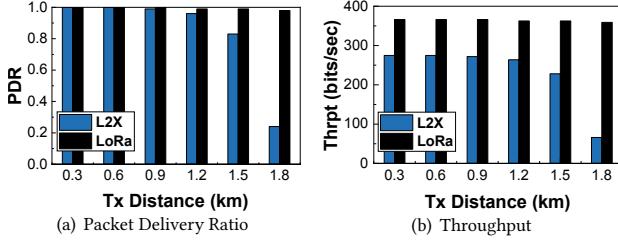


Figure 20: PDR and Throughput of L2X with different distances between the reference and the data transmitters.

a very low data rate. L2X outperforms all other methods in both SER and throughput. Figure 19 shows L2X’s performance in the outdoor campus-scale deployment. LoRaBee fail to work for most locations in this outdoor deployment due to its high SNR requirement for demodulation. Thus, we only present the comparison of L2X and FreeBee for the outdoor experiment. L2X detect all packets transmitted at the 13 locations, which verifies the efficiency of our packet detection method. Figure 19(a) illustrates that the SER increases as the distance increases. As an exception, the receiver at location 12 is close to the transmitters, but it has a high SER due to the heavy blockage and interference by a nearby laboratory building. L2X decreases the SER by upto 29% than FreeBee. Besides, as L2X encodes more bits for each chirp symbol, the network throughput of L2X is about 9 \times to 31 \times of that of FreeBee.

Figure 20 shows the impact of distance between reference and data transmitters on L2X performance. We take the native LoRa as the baseline by setting a LoRa receiver co-located with the L2X receiver. Figure 20(a) shows the PDR of L2X , where most packets are successfully decoded even when the distance between transmitters reaches 1.2km. This also shows the benefit that the propagation time offset is compensated by taking the preamble frequencies as a reference. As the distance increases to 1.8km, the PDR of L2X decreases due to the signal attenuation of long-range links. Figure 20(b) shows the throughput of L2X. L2X has a high throughput even when the two transmitters are 1.2km distance away, due to the propagation offset compensation. The native LoRa has a higher throughput than L2X , but it requires both the transmitter and the receiver supports the LoRa protocol, limiting its usage.

10.4 Wi-Fi and Bluetooth Rx

Setup: We evaluate the performance of L2X with Wi-Fi and Bluetooth receivers in 2.4GHz bands. We implement L2X receivers on commercial off-the-shelf Bluetooth devices (TI CC2652R [20]) and Wi-Fi devices (Intel 5300 NIC [31]). The sampling rate of the Bluetooth receiver is 25kHz due to clock restrictions of low-cost hardware. We use the CSITool software platform [27] installed on the Wi-Fi devices for collecting RSSI readings. The CSITool platform requires the Wi-Fi receiver associated to an AP. Thus, it can collect RSSI readings based on the periodical probes from the AP. The duration of a Wi-Fi probe is much shorter than a LoRa chirp. Therefore, we can collect many RSSI samples on each LoRa chirp for L2X demodulation. In our experiment, the sampling rate of the CSITool is set at 2kHz, where the probe interval is 0.5ms with a packet length of 145 bytes. We use 2.4G LoRa devices with SX1280 [26] chips for transmitting LoRa packets. The duration of a LoRa chirp

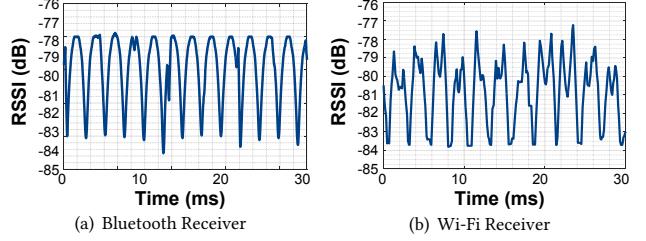


Figure 21: RSSI readings of the L2X signal at Bluetooth (TI CC2652R) and Wi-Fi (Intel 5300 NIC) receivers.

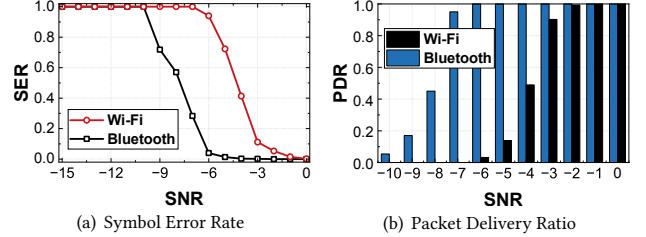


Figure 22: SER and PDR on Wi-Fi and Bluetooth receivers.

is 20ms with the SF configuration of 12 and BW= 203.125kHz. The experiment is carried out in the indoor environment. We use a USRP N210 to continually generate Gaussian noise to change the received SNR on demand. The received SNR is estimated with a native LoRa receiver that is co-located with the L2X receiver. The noise in the Wi-Fi experiments includes both the channel noise and the concurrent Wi-Fi probe signals.

Results: Figure 21 shows the RSSI readings at Bluetooth and Wi-Fi receivers. We can see that both signals follow the varying amplitude pattern. We can also see more severe distortion in the Wi-Fi RSSI readings compared with that of the Bluetooth. This is because the Wi-Fi bandwidth is much wider than that of the Bluetooth, and thus it introduces much more in-band noise in RSSI readings. Besides, the sampling rate of the Wi-Fi receiver (i.e., 2kHz) is much lower than that of the Bluetooth (i.e., 25kHz) due to restrictions of commodity Wi-Fi NIC interfaces, which further exacerbates the distortion of Wi-Fi RSSI waveforms. Figure 22(a) shows the SER of L2X at Wi-Fi and Bluetooth receivers with different SNRs. The SERs of the two receivers first keep low, and then grow as the SNR decreases to the demodulation threshold. The SER of the Wi-Fi receiver increases faster than that of the Bluetooth due to the noise distortion and low sampling rate of the commodity Wi-Fi device. Figure 22(b) presents the PDR for the two receivers on decoding LoRa packets. Both receivers can decode more than 99% of LoRa transmissions when the SNR is above -2dB. The Bluetooth receiver can still decode 95% of LoRa packets even when the LoRa SNR is as low as -7dB. Based on previous evaluations of 2.4GHz LoRa communication ranges in outdoor city-scale environments [32], the RSSI of native LoRa decreases rapidly as the communication range increases, which is -85dBm on 0.6km, -96dBm on 1.2km, and -120dBm on 2.7km given the noise floor of -85dBm. We derive the SNR-distance relationship based on the RSSI estimations. The expected PDR for the BLE L2X receiver can be higher than 99% when the distance is within 900m. Then the PDR decreases rapidly after 900m and becomes zero as the communication range increases over 1.2km. The expected PDR of Wi-Fi L2X is about 95% when the

communication range is at 300m and quickly decreases to zero as the distance increases. L2X communication with Wi-Fi devices degrades significantly in the wild deployments as the wide bandwidth of Wi-Fi introduces much more noise. For the future work, we can improve the performance of L2X Wi-Fi receivers by applying a small bandwidth with the latest MU-OFDMA technique.

11 DISCUSSION

In this section, we briefly discuss some design issues of L2X.

- **Security.** L2X leverages the same security mechanism with the native LoRa, where it implements end-to-end encryption for application payloads exchanged between end-devices and application servers. L2X transmitters encrypt data bits in the application layer. Thus, even attackers can decode the physical layer symbols, they cannot recover the application data.

- **Deployment Cost.** L2X leverages two cooperative LoRa devices for packet transmission. In practice, two LoRa transmitters in L2X can serve many non-LoRa IoT devices in a large coverage area. This reduces the cost for deploying transmitters considering the scale of the whole network. Besides, L2X can also take the mandatory LoRaWAN beacons from gateways as the reference signal. In such a case, the reference node does not introduce extra overhead and the deployment cost for L2X transmitters will be further reduced.

- **Packet Collisions.** There will be packet collisions when multiple LoRa data nodes send packets simultaneously. However, as LoRa chirps with different SF and bandwidth configurations are orthogonal to each other, concurrent LoRa packets of different SFs are not de-spreaded during the transmission, and thus they introduce little impact on the L2X demodulation. For concurrent LoRa transmissions with the same SF and bandwidth, we can adopt LoRa collision resolving approaches for recovering the data packet from the interfering signal [24]. For example, we can distinguish FFT peaks of data packets from interference based on their power difference.

- **Robustness to Interference.** L2X is more susceptible to interference (e.g., Wi-Fi interference in 2.4GHz) than the native LoRa. Wireless interference alongside LoRa transmissions has an impact on the RSSI of the L2X receiver. Unexpected RSSI changes within a LoRa transmission can lead to L2X demodulation errors. Besides, L2X receivers on COTS Wi-Fi hardware have a wider receiving bandwidth than the LoRa BW, which leads to more in-band interference than the native LoRa. Based on the analysis of Sec. 8, the SNR_{data} and SNR_{ref} in Eq. 13 should be at least 7.1dB for L2X demodulation with Wi-Fi receivers. The lowest requirements for SNR_{data} and SNR_{ref} are each increased by 19.9dB due to the wider Wi-Fi bandwidth compared with LoRa (i.e., 20MHz versus 203.125kHz). A possible improvement can be using the MU-OFDMA in Wi-Fi 6 to acquire one single RU with the minimum receiving bandwidth of 2MHz. Decoding LoRa packets against interference will be our future work.

12 RELATED WORKS

Cross-Technology Communication. Much research effort has been made on cross-technology communication (CTC) for heterogeneous wireless technologies. Previous CTC works mainly focus on the interconnection between short-range wireless, e.g., Wi-Fi, Bluetooth, and ZigBee, by exploiting the packet-level information [2–4]

or physical-layer signal emulation [7–9]. Packet-level CTC leverages packet characteristics such as signal strength [3–6], transmission time [2, 33, 34], and packet length [35] for conveying data. Those approaches suffer from low bit rate as each packet only modulates several bits. Physical-layer CTC improves the communication efficiency via signal emulation [7, 8, 10–13, 36–38]. The key idea is to use high-end transmitters (e.g., Wi-Fi APs) to emulate low-end device compliant packets (e.g., Bluetooth and ZigBee) by manipulating payloads of transmitting packets. LTE2B [13] connects ZigBee devices with licensed LTE through physical-layer signal emulation with a communication range of upto 400 m. Recent research explores interconnecting between short-range wireless and LPWANs. LoRaBee [14] pushes LoRa packets to ZigBee by detecting RSSI at the ZigBee device. It sets the LoRa channel to partially overlap with the ZigBee band. Thus, the frequency-varying LoRa chirps lead to RSSI changes at the receiver, which can be used for demodulation. XFi [15] decodes LoRa packets at a Wi-Fi receiver by recovering chirp signals from the Wi-Fi CSI trace. Those works do not leverage the LoRa CSS modulation for energy concentration and cannot decode low-SNR LoRa signals. Different from those works, L2X de-spreads chirps for energy aggregation to achieve reliable long-range CTC.

Concurrent LoRa transmission. L2X is motivated by extensive works on decoding concurrent LoRa transmissions. They resolve signal collisions by leveraging LoRa physical features such as hardware imperfections [39, 40], temporal signal characteristics [41–43], energy distributions [44–46] and frequency domain features [24, 47]. These works boost channel efficiency by tackling multiple challenges of high transmitter concurrency, real time processing, bad channel conditions and so on. L2X leverages the physical features of concurrent LoRa transmissions for decoding LoRa packets at non-LoRa receivers, and thus achieving reliable long-range CTC.

13 CONCLUSION

This paper proposes L2X to provide long-range CTC for diverse wireless receivers over LoRa. The key innovation of L2X is an energy-concentrating demodulation mechanism that de-spreads LoRa chirps over the air. Therefore, L2X enables non-LoRa receivers to detect and demodulate LoRa signals even under extremely low SNRs. We propose several novel techniques to address practical challenges. We design a method for LoRa signal detection and synchronization based on the structure of the preamble. We maximize the receiving sensitivity with a cross-domain demodulation approach. We implement L2X on COTS devices and thoroughly evaluate its performance with both indoor and outdoor deployments. The evaluation results show that L2X can achieve 1.2 km long-distance CTC to diverse receivers with an extremely low SNR of -9 dB, improving the distance by 30× compared with the state-of-the-art LoRaBee method.

ACKNOWLEDGMENT

We thank the anonymous shepherd and reviewers for their insightful comments to improve the quality of our work. This work is in part supported by NSFC No. 62172250, No. 61932013, Tsinghua University Initiative Scientific Research Program. Jiliang Wang is the corresponding author.

REFERENCES

- [1] Statista Research Department. Internet of things (iot) connected devices installed base worldwide from 2015 to 2025. 2016.
- [2] Song Min Kim and Tian He. Freebee: Cross-technology communication via free side-channel. In *Proceedings of ACM MobiCom*, 2015.
- [3] Xiuzhen Guo, Yuan He, and Xiaolong Zheng. Wizig: Cross-technology energy communication over a noisy channel. *IEEE/ACM Transactions on Networking*, 28(6):2449–2460, 2020.
- [4] Xiuzhen Guo, Yuan He, Xiaolong Zheng, Liangcheng Yu, and Omprakash Gnawali. Zifgi: Harnessing channel state information for cross-technology communication. *IEEE/ACM Transactions on Networking*, 28(1):301–311, 2020.
- [5] Xiaolong Zheng, Yuan He, and Xiuzhen Guo. Stripcomm: Interference-resilient cross-technology communication in coexisting environments. In *Proceedings of IEEE INFOCOM*, 2018.
- [6] Kameswari Chebolu and Ashutosh Dhekne. Esense: Communication through energy sensing. In *Proceedings of ACM MobiCom*, 2009.
- [7] Zhijun Li and Tian He. Webbee: Physical-layer cross-technology communication via emulation. In *Proceedings of ACM MobiCom*, pages 2–14, 2017.
- [8] Hsun-Wei Cho and Kang G Shin. Bluefi: bluetooth over wifi. In *Proceedings of ACM SIGCOMM*, pages 475–487, 2021.
- [9] Xiuzhen Guo, Yuan He, Xiaolong Zheng, Zihao Yu, and Yunhao Liu. Legofifi: Transmitter-transparent ctc with cross-demapping. *IEEE Internet of Things Journal*, 8(8):6665–6676, 2021.
- [10] Xiuzhen Guo, Yuan He, Jia Zhang, and Haotian Jiang. Wide: Physical-level ctc via digital emulation. In *2019 18th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pages 49–60. IEEE, 2019.
- [11] Wenchao Jiang, Zhimeng Yin, Ruofeng Liu, Zhijun Li, Song Min Kim, and Tian He. Bluebee: a 10,000 × faster cross-technology communication via phy emulation. In *Proceedings of ACM SenSys*, 2017.
- [12] Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, and Tian He. Wibeacon: expanding ble location-based services via wifi. In *Proceedings of ACM MobiCom*, Online, 2021.
- [13] Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, and Tian He. Lte2b: Time-domain cross-technology emulation under lte constraints. In *Proceedings of ACM SenSys*, New York, NY, USA, 2019.
- [14] Junyang Shi, Di Mu, and Mo Sha. Lorabee: Cross-technology communication from lora to zigbee via payload encoding. In *Proceedings of IEEE ICNP*, pages 1–11. IEEE, 2019.
- [15] Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, and Tian He. Xfi: Cross-technology iot data collection via commodity wifi. In *Proceedings of IEEE ICNP*, pages 1–11. IEEE, 2020.
- [16] Chennling Li and Zhichao Cao. Lora networking techniques for large-scale and long-term iot: A down-to-top survey. *ACM Comput. Surv.*, 55(3), feb 2022.
- [17] Yinghui Li, Jing Yang, and Jiliang Wang Wang. Dylora: Towards energy efficient dynamic lora transmission control. In *Proceedings of IEEE INFOCOM*, Online, July 6–9, 2020.
- [18] Zhenqiang Xu, Pengjin Xie, Shuai Tong, and Jiliang Wang. From demodulation to decoding: Towards complete lora phy understanding and implementation. *ACM Trans. Sen. Netw.*, jun 2022. Just Accepted.
- [19] Semtch. Sx1276/77/78/79 datasheet [online]. Available: <https://www.semtech.com/products/wireless-rf/lora-core/sx1278>. Accessed: Mar.20, 2022.
- [20] Texas Instruments. Cc2652r datasheet [online]. Available: <https://www.ti.com/product/CC2652R>. Accessed: Mar.20, 2022.
- [21] Chaojie Gu, Rui Tan, and Xin Lou. One-hop out-of-band control planes for multi-hop wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 15(4):1–29, 2019.
- [22] Jing Yang, Zhenqiang Xu, and Jiliang Wang. Ferrylink: Combating link degradation for practical lpwan deployments. In *2021 IEEE 27th International Conference on Parallel and Distributed Systems (ICPADS)*, pages 575–582. IEEE, 2021.
- [23] Lifyand E. Hilbert Transform. In: *Harmonic Analysis on the Real Line. Pathways in Mathematics*. Birkhäuser, Cham, 2021.
- [24] Shuai Tong, Jiliang Wang, and Yunhao Liu. Combating packet collisions using non-stationary signal scaling in lpwans. In *Proceedings of ACM MobiSys*, Toronto, Canada, June 16–19, 2020.
- [25] Shuai Tong, Zilin Shen, Yunhao Liu, and Jiliang Wang. Combating link dynamics for reliable lora connection in urban settings. In *Proceedings of ACM MobiCom*, New York, NY, USA, 2021.
- [26] Semtch. Sx1280 datasheet [online]. Available: <https://www.semtech.com/products/wireless-rf/lora-24ghz/sx1280>. Accessed: Mar.20, 2022.
- [27] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. Tool release: Gathering 802.11n traces with channel state information. *ACM SIGCOMM CCR*, 41(1):53, Jan. 2011.
- [28] USRP Ettus. N210 datasheet. Available: <https://www.ettus.com/>.
- [29] Texas Instruments. Cc1310 datasheet [online]. Available: <https://www.ti.com/product/CC1310>. Accessed: Mar.20, 2022.
- [30] Monsoon Solutions Inc. High voltage power monitor. Available: <https://www.msoon.com/high-voltage-power-monitor>.
- [31] Intel. Intel ultimate n wifi link 5300 datasheet [online]. Available: <https://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/ultimate-n-wifi-link-5300-brief.pdf>. Accessed: Aug.2, 2022.
- [32] Zheng Zhang, Shouqi Cao, and Yuntengyao Wang. A long-range 2.4 g network system and scheduling scheme for aquatic environmental monitoring. *Electronics*, 8(8):909, 2019.
- [33] Wenchao Jiang, Zhimeng Yin, Song Mim Kim, and Tian He. Transparent cross-technology communication over data traffic. In *Proceedings of IEEE INFOCOM*, 2017.
- [34] Zhimeng Yin, Wenchao Jiang, Song Min Kim, and Tian He. C-morse: Cross-technology communication with transparent morse coding. In *Proceedings of IEEE INFOCOM*, 2017.
- [35] Yifan Zhang and Qun Li. Howies: A holistic approach to zigbee assisted wifi energy savings in mobile devices. In *Proceedings of IEEE INFOCOM*, 2013.
- [36] Yongrui Chen, Zhijun Li, and Tian He. Twinbee: Reliable physical-layer cross-technology communication with symbol-level coding. In *Proceedings of IEEE INFOCOM*, 2018.
- [37] Zhijun Li and Tian He. Longbee: Enabling long-range cross-technology communication. In *Proceedings of IEEE INFOCOM*, 2018.
- [38] Zhijun Li and Yongrui Chen. Bluefi: Physical-layer cross-technology communication from bluetooth to wifi. In *Proceedings of IEEE ICDCS*, 2020.
- [39] Rashad Eletreby, Diana Zhang, Swarun Kumar, and Osman Yağan. Empowering low-power wide area networks in urban settings. In *Proceedings of ACM SIGCOMM*, Los Angeles, CA, USA, August 21–25, 2017.
- [40] Zhenqiang Xu, Shuai Tong, Pengjin Xie, and Jiliang Wang. Fliplora: Resolving collisions with up-down quasi-orthogonality. In *Proceedings of IEEE SECON*, Online, June 22–25, 2020.
- [41] Xiong Wang, Linghe Kong, Liang He, and Guihai Chen. mIora: A multi-packet reception protocol for lora communications. In *Proceedings of IEEE ICNP*, Chicago, Illinois, USA, October 7–10, 2019.
- [42] Zhe Wang, Linghe Kong, Kangjie Xu, Liang He, Kaishun Wu, and Guihai Chen. Online concurrent transmissions at lora gateway. In *Proceedings of IEEE INFOCOM*, Online, July 6–9, 2020.
- [43] Xia Xianjin, Zheng Yuanqing, and Gu Tao. Ftrack: Parallel decoding for lora transmissions. In *Proceedings of ACM SenSys*, New York, NY, USA, November 10–13, 2019.
- [44] Bin Hu, Zhimeng Yin, Shuai Wang, Zhuqing Xu, and Tian He. Sclora: Leveraging multi-dimensionality in decoding collided lora transmissions. In *Proceedings of IEEE ICNP*, Online, October 13–16, 2020.
- [45] Zhenqiang Xu, Pengjin Xie, and Jiliang Wang. Pyramid: Real-time lora collision decoding with peak tracking. In *Proceedings of IEEE INFOCOM*, Online, May 10–13, 2021.
- [46] Qian Chen and Jiliang Wang. Aligntrack: Push the limit of lora collision decoding. In *Proceedings of IEEE ICNP*, pages 1–11, 2021.
- [47] Shuai Tong, Zhenqiang Xu, and Jiliang Wang. Colora: Enabling multi-packet reception in lora. In *Proceedings of IEEE INFOCOM*, Online, July 6–9, 2020.