Wi−Lo: Emulation of LoRa using Commodity 802.11b WiFi Devices

Piotr Gawłowicz, Anatolij Zubow, Falko Dressler
Technische Universität Berlin, Germany
{gawlowicz, zubow, dressler}@tkn.tu-berlin.de

***Abstract*—The recent move of LoRa towards the unlicensed 2.4 GHz ISM spectrum band creates multiple opportunities for its broader usage in new IoT applications. However, the ISM band is already highly populated with diverse wireless systems, and interference issues are expected. We believe that cross-technology communication (CTC) can help to speed up LoRa adaptation and mitigate the coexistence problems. Therefore, in this paper, we introduce `Wi−Lo`, a novel signal emulation-based CTC approach, which allows a WiFi device to generate a valid LoRa waveform. Our scheme requires no hardware modifications but depends only on the careful selection of WiFi frame payload bits. We build our `Wi−Lo` prototype with commodity hardware. Our evaluation reveals that `Wi−Lo` enables reliable communication from WiFi to LoRa devices, which is comparable to the configurations using native LoRa nodes. Moreover, by leveraging the high link budget of LoRa, a long distance CTC can be established.**

***Index Terms*—WiFi, LoRa, CTC, Signal Emulation, COTS**

I. Introduction

Today, we see a constant growth in the number of connected devices forming the Internet of Things (IoT) idea. Low-power wide area networks (LPWANs) are an attractive way to connect such a large number of IoT devices. Long Range Wide Area Network (LoRa) [1] becomes a widely used technology, which attracts many interests from research and academia. Initially, LoRa was designed to operate in the sub-gigahertz bands, however, recently it started using also the globally available 2.4 GHz industrial, scientific and medical (ISM) band (so-called 2.4 GHz LoRa) [2]. The key benefit is the larger available spectrum in 2.4 GHz band (i.e., 80 MHz compared to only a few MHz in sub-GHz), which allows operating multiple LoRa channels in parallel and relax the strict requirement for channel duty cycling. Moreover, the maximum bandwidth is increased to 1.625 MHz, resulting in a higher data rate and hence allowing LoRa to support a wider range of IoT applications.

Despite the described advantages, the move towards 2.4 GHz band also brings a new opportunity of employing the Cross-Technology Communication (CTC) to speed up the adaptation, popularity and usage of LoRa protocol while deploying only a fraction of otherwise required LoRa devices. CTC builds direct communications across heterogeneous wireless technologies, which removes the need for multi-radio gateways and therefore avoids their drawbacks (e.g., hardware cost, deployment complexity, or increasing wireless traffic). Specifically, by applying the CTC concepts, we can enable ubiquitously deployed wireless devices to emulate the LoRa signal and repurpose them in long-range IoT applications (e.g., maintenance notification, disaster communications). The CTC was already enabled between LoRa and ZigBee [3], [4] as well as LoRa and Bluetooth [4], [5].

This work was supported in part by the Federal Ministry for Economic Affairs and Climate Action (BMWK, Germany) within ZIM Programme under Grant 16KN073726 and by the Federal Ministry of Education and Research (BMBF, Germany) within the 6G Research and Innovation Cluster 6G-RIC under Grant 16KISK020K.

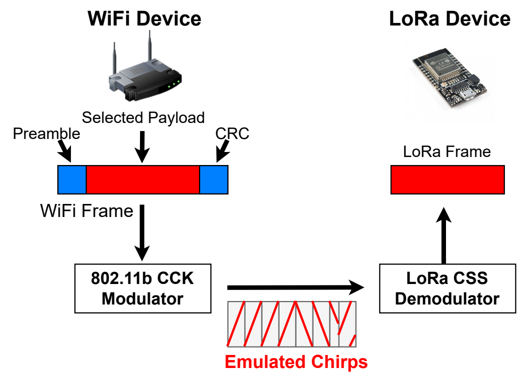

Fig. 1: Overview of `Wi−Lo`.

In this paper, we present `Wi−Lo` , which uses signal emulation technique to make commodity 802.11 WiFi hardware able to generate a valid 2.4 GHz LoRa waveform (cf. Figure 1). We envision multiple applications of `Wi−Lo`, e.g., reduction of cross-technology interference (CTI) by explicit channel access coordination (i.e., WiFi can reserve channel airtime using RTS/CTS mechanism and notify the neighboring LoRa node about transmission opportunity over the CTC channel). With `Wi−Lo` WiFi-based sensors can report their measurement data to a LoRa base station within only one hop. Finally, as we will demonstrate the emulated LoRa signal provides a much longer communication distance than a WiFi signal, therefore, WiFi networks can use `Wi−Lo` as a backup communication method. Note that a complementary scheme called XFi [6] enables WiFi AP to receive LoRa signal.

Our main contributions can be summarized as follows:

- We present `Wi−Lo`, a novel long-range signal emulation-based CTC scheme from WiFi to LoRa. The unique design of `Wi−Lo` lies in chirp emulation, i.e., generating a specific WiFi signal approximating desired LoRa chirps only by payload selection. `Wi−Lo` requires no hardware modification and is transparent to both technologies.
- We show how to synthesize a valid LoRa frame under the constraints of 802.11b physical layer, and that we

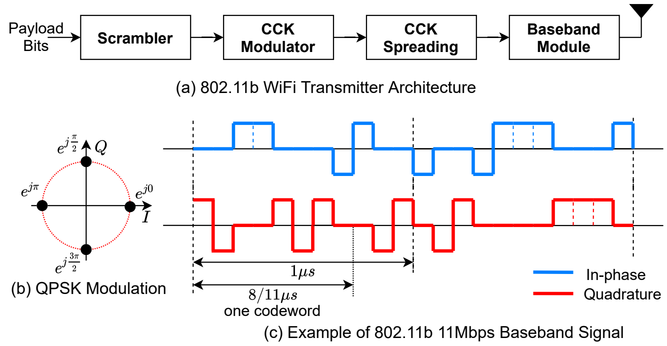

Fig. 2: 802.11b WiFi transmitter architecture (a), QPSK constellation diagram (b), and example CCK baseband signal (c).

can emulate multiple LoRa channels inside a single WiFi frame.

- We implement Wi-Lo on commodity devices, i.e., we use WiFi Atheros AR928x card and LoRa evaluation kit from Semtech (WiMOD). Our evaluations reveal that Wi-Lo achieves almost the same performance as standard LoRa transmissions, i.e., the SNR loss due to signal emulation at most 5 dB. Wi-Lo enables CTC between WiFi and LoRa with the maximal LoRa data rate of 253.91 kbps with almost 100% frame reception rate. The transmission distance is more than 300 meters, dramatically outperforming native WiFi communication.

II. Background

This section gives relevant information on the IEEE 802.11b and 2.4 GHz LoRa technology.

A. IEEE 802.11b Primer

Fig. 2 shows an overview of the 802.11b transmitter that operates as follows. *i)* WiFi scrambles incoming payload by XORing the bits with the output of a 7-bit linear feedback shift register[1]. *ii)* The transmitter performs CCK modulation and spreading. *iii)* The waveform is converted to analog signal, shifted to the carrier frequency and sent through an antenna.

Fig. 3 shows the details of the CCK scheme for a data rate of 11 Mbps, where 8 bits are transmitted per 8-chip codeword (i.e., chip rate of 11 Mchips/s). Here, each pair of bits is used to determine four phases ϕ_i. The first two bits (i.e., $d_0 d_1$) encode ϕ_1 based on DQPSK. The phase change for ϕ_1 is relative to the phase ϕ_1 of the preceding codeword. In addition, the phase ϕ_1 in all odd-numbered codewords of the payload are given an extra 180° rotation. The next three pairs of bits encode ϕ_2, ϕ_3 and ϕ_4 based on QPSK. The following formula is used to derive the CCK codewords to spread both 5.5 and 11 Mbps:

$$\begin{aligned}\mathbf{c} =&(c_0, \dots, c_7)\\ =&(e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_4)},\\ &-e^{j(\phi_1+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_3)}, e^{j(\phi_1+\phi_3)}, -e^{j(\phi_1+\phi_2)}, e^{j\phi_1})\end{aligned}$$

Note that in the CCK scheme, DQPSK and QPSK modulations assign only phases $\phi_i \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. Then, during the CCK spreading, the phases of each chip in a CCK codeword are computed as a linear combination of ϕ_i. Consequently, each chip can be represented as $e^{j\varphi}$, where $\varphi \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. Therefore, the phase changes by up to $\frac{3\pi}{2}$ at most every $\frac{1}{11}\mu s$. The details of the CCK can be found in 802.11 standard [7].

[1]The scrambling seed is fixed to [1101100] in the standard.

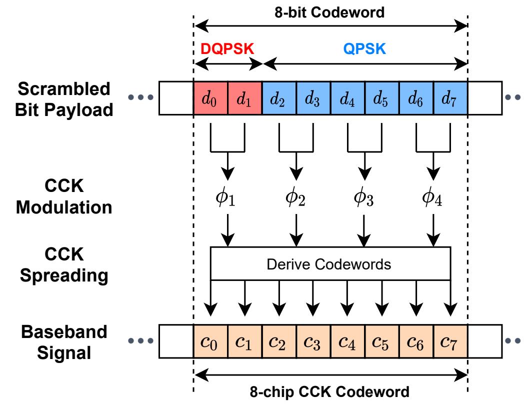

Fig. 3: 802.11b CCK scheme for data rate of 11 Mbit/s.

B. LoRa PHY in 2.4 GHz

LoRa is a proprietary LPWAN technology developed by Semtech [8]. It employs the chirp spread spectrum (CSS) technique to modulate data. A chirp in CSS refers to a signal with constantly increasing (i.e., up-chirp) frequency that sweeps through and wraps around a predefined bandwidth BW (i.e., between $-\frac{BW}{2}$ to $+\frac{BW}{2}$) over time T [9]. The base up-chirp $C(t)$ is represented as

$$C(t) = e^{j2\pi(-\frac{BW}{2}+\frac{kt}{2})t}$$

where $k = \frac{BW}{T}$ is the gradient of frequency sweeping. Such chirps are robust against interference, noise and other negative channel effects, and hence they can be detected and decoded even under extremely low SNR values.

CSS modulates data by shifting the starting frequency of a base up-chirp, i.e., the starting position encodes the value of the symbol. Given the frequency shift f, the shifted chirp is $C(t)e^{j2\pi ft}$. LoRa defines $M = 2^{SF}$ different frequency shifts, that result in M uniformly spaced up-chirps to encode SF bits. SF is the spreading factor that controls the chirp rate. The chirp duration is given by $T_S = M/BW$. Therefore, increasing SF by one allows encoding one more bit and doubles the chirp duration making the transmission slower but more robust against errors.

Fig. 4 illustrates the structure of a LoRa frame. As shown, the frame starts with a preamble consisting of a variable number of base up-chirps, then a sync word of two base up-chirps

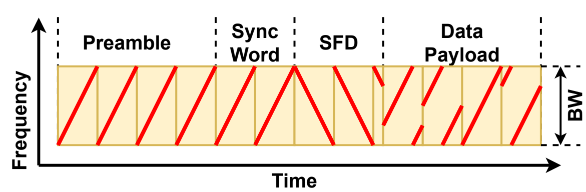

Fig. 4: Structure of LoRa Frame.

and 2.25 down-chirp denoted as Start Frame Delimiter (SFD) for chirp-level synchronization. Then, the payload (including optional header) chirps follows.

The LoRa receiver detects a frame by exploiting the repeating property of its preamble. Then, it localizes the start point of the SFD for accurate chirp synchronization. From this point, the receiver divides the received signal into segments corresponding to chirps and demodulates them individually. The demodulation procedure is illustrated in Fig. 5. In particular, the receiver multiplies each received chirp with a complex conjugate of the base up-chirp $C^*(t)$ (i.e., down-chirp) and performs Fast Fourier Transform (FFT) operation. The first operation results in a single tone at frequency f as:

$$C^*(t) \times C(t)e^{j2\pi ft} = e^{j2\pi ft}$$

Therefore, the data demodulation is based on localizing a bin with the energy peak in the result of the Fourier transformation. The index of the bin represents the encoded data of the corresponding chirp.

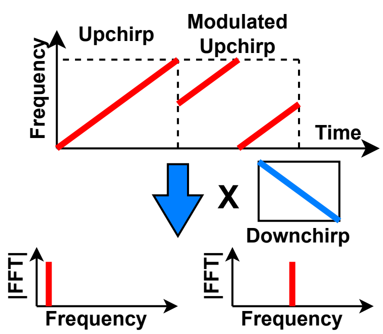

Fig. 5: Demodulation of CSS.

Recently, Semtech released a LoRa chipset operating at 2.4 GHz to enter the globally available unlicensed ISM band. The 2.4 GHz LoRa is based on sub-GHz Lora. In addition, it supports wider bandwidth (i.e., up to 1625 kHz vs. 500 kHz) and lower SF values, which result in higher data rates.

III. Wi-Lo

A. *Wi-Lo in a Nutshell*

Fig. 1 illustrates how `Wi-Lo` works: a WiFi device transmits a frame with carefully selected payload bits so that the CCK modulation generates a sequence of emulated LoRa chirps, i.e., the waveform is recognized by a LoRa receiver as a valid LoRa frame. Specifically, based on reverse engineering of the 802.11b TX chain, `Wi-Lo` constructs the payload of a WiFi frame. On the forward TX path, the payload is spread into chips and transmitted as a wide-band signal. When this signal flows into the LoRa receiver, it passes the low pass filter (LPF) and successfully triggers a standard LoRa RX procedure. Note that the content of WiFi preamble, header and trailer cannot be controlled, hence it cannot be used to generate desired signals. A LoRa receiver ignores those parts and treats them as noise.

B. *LoRa Chirp Emulation with 802.11b CCK*

To achieve the signal emulation on real WiFi and LoRa devices using chirp emulation, we must take into account the physical layer constraints of both technologies. Specifically, when an emulated chirp is transmitted by WiFi, both its frequency range and its time duration has to match with the target LoRa chirp. A chirp with a spreading factor of SF has 2^{SF} samples, while the sampling rate equals its bandwidth BW. For example, when $SF = 7$ and $BW = 1625\,kHz$, the duration of an emulated chirp is given by:

$$T_{chirp} = \frac{2^{SF}}{BW} = \frac{128}{1625\,kHz} \approx 79\mu s$$

WiFi (802.11b) device uses the chip rate of 11 Msym/s (i.e., the chip duration equals $\frac{1}{11}\mu s$). Therefore, a WiFi has to transmit $79/(1/11) = 869$ chips to generate a waveform with a duration of a single LoRa chirp. For CCK modulation in the 11 Mbps mode, one payload bit is modulated into one CCK chip, and thus 869 bits are utilized to emulate a LoRa chirp.

Let's temporarily assume that the CCK modulator does not have any constraints, i.e., it can arbitrarily generate a sequence of valid QPSK chips. Then, by properly selecting the chip sequence, we can reduce the rate of phase changes, and hence impact the frequency of the output waveform. Specifically, we can set the phase of multiple consecutive chips to be the same. Following this observation, the CCK modulator can be used as a Pulse-width modulation (PWM) based signal source capable of generating any signal with frequency components up to 11 MHz.

Unfortunately, two challenges are preventing the straightforward approach. First, the CCK scheme generates codewords (i.e., a group of 8 chips) whose phases are not independent. In particular, the CCK codebook contains only 256 valid codewords, which violates our assumption of being able to produce arbitrary QPSK sequences. Note that if a phase of each chip could be set independently, the codebook would have a size of $4^8 = 65536$. Second, the LoRa waveform is a complex signal with In-phase (I) and Quadrature (Q) components, that need to be generated correctly by two PWM modulators. Unfortunately, the CCK modulator cannot arbitrarily and independently set the I and Q components. Specifically, in QPSK, when the I component has a non-zero value, the Q equals zero and vice-versa.

To overcome the constraints of the CCK modulator without modifying the WiFi device, we exploit two facts: *i)* the bandwidth of the LoRa signal is much smaller than the bandwidth of the WiFi (i.e., up to 1.625 MHz vs. 22 MHz), *ii)* a LoRa receiver performs low-pass filtering for noise reduction. The LPF removes components above 1.625 MHz from the WiFi signal, which has the same effect as averaging the input signal in the time domain. Our key insight is that even with the present constraints, we can still create a PWM-like signal by correctly selecting CCK codewords so that the filtered CCK signal closely approximates the complex LoRa signal. To this end, we propose the following emulation approach.

First, we generate the entire LoRa waveform S and oversample the signal with a rate of 11 MHz. As the signal is approximated with CCK codewords, we divide the signal S into chunks s of $\Delta t = \frac{8}{11}\,\mu$s duration. Next, for each chunk

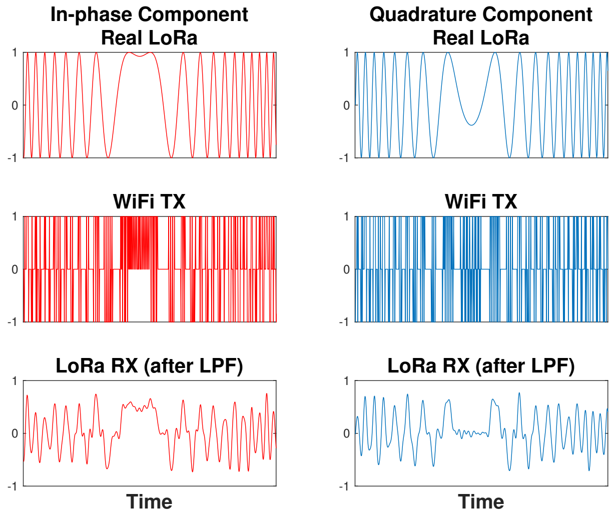

Fig. 6: Emulation overview: real LoRa up-chirp, WiFi waveform and signal received by LoRa device (after LPF).

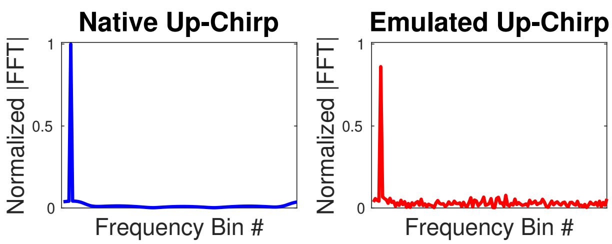

Fig. 7: Demodulation of real and emulated LoRa up-chirp.

s, we look for a CCK symbol $\tilde{c} \in C_{\text{cck}}$ that is closest to the desired sequence. We define the quality of approximation as:

$$\tilde{c} = \underset{c \in C_{\text{cck}}}{\text{argmax}}\, \Re(s) * \Re(c) + \Im(s) * \Im(c)$$

where $C_{\text{cck}} \in \{\text{spread}(\text{perms}([0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}]))\}$, $\text{perms}(\cdot)$ computes the permutations, $\text{spread}(\cdot)$ is the CCK spreading, $*$ is cross-correlation and $\Re()$ and $\Im()$ represent the real and imaginary part of the complex signal. We append the $\tilde{c}$ to the sequence $\tilde{C}$, that stores the LoRa signal approximated by the CCK codewords. Based on inverting the WiFi TX chain, we derive a WiFi frame payload P from the $\tilde{C}$.

The results in Fig. 6 prove that the proposed emulation is feasible. We observe that the imperfections due to signal emulation are smoothed out by the moving average effect of the LPF, and the emulated LoRa up-chirp looks very similar to the real up-chirp signal in the time domain. Although the filtered signal is still distorted, the result Fig. 7 shows that during the standard LoRa demodulation the emulated signal leads to the same peak as the native up-chirp, thus it can be successfully decoded at a LoRa receiver. Moreover, the distortions of the emulated signal lead to a very small degradation of the magnitude of the FFT peak. Therefore, `Wi-Lo` can potentially achieve a similar link performance as the standard LoRa.

C. Multi-Channel Communication

Semtech proposed that LoRa devices in 2.4 GHz band shall be capable of operating in the 2400 MHz to 2480 MHz frequency band with channels spaced equally by 200 Hz [10]. Contrary, WiFi defines 14 overlapping channels spaced with 5 MHz step starting from 2412 MHz. Therefore, we expect that very often the central frequencies of LoRA channels will not coincide with any WiFi channel.

We find that when a WiFi transmitter operates at the center frequency f_W, while LoRa receiver observes the WiFi signal from a different center frequency f_L, `Wi-Lo` can shift the LoRa signal in the frequency domain by $\Delta f = f_W - F_L$. This can be achieved by the dot-product of the LoRa signal with a digital carrier $e^{j\Delta ft}$. Then, `Wi-Lo` successfully follows the proposed emulation scheme to generate a LoRa transmission centred at any frequency within the WiFi channel bandwidth.

Following this approach, we can multiplex multiple LoRa waveforms (at different frequencies) to be emulated and transmitted during a single WiFi frame. This way, we enable concurrent LoRa transmissions, and hence improve the efficiency of the `Wi-Lo`, i.e., we increase the total data rate of LoRa transmissions emulated in a wideband WiFi waveform.

IV. Performance Evaluation

We have implemented `Wi-Lo` prototype using commodity WiFi (Atheros AR928x) and LoRa (Semtech SX1280) hardware. Note that `Wi-Lo` is not hardware-specific, i.e., it works with any WiFi hardware as it uses only standard 802.11b frame transmission. The payload of WiFi frames is precomputed using Matlab WLAN Toolbox. In addition, we use a USRP B205-mini to generate real and emulated LoRa frames from the same device for signal quality comparison purposes.

The LoRa payload size is selected appropriately to fit into a maximal WiFi frame payload (i.e., 2.98 ms). As 12.25 LoRa chirps are needed for the first part of the frame (i.e., preamble, etc.), we used only pairs of SF and BW, which allow creating at least 15 LoRa chirps within the WiFi frame. For example, with $SF = 5$ and $BW = 1625\, kHz$, we can create 150 chirps and achieve a data rate of 253.91 kbps. The channel frequency is set to 2427 MHz, which corresponds to channel 6 in WiFi. We used the LoRa device in a sniffer mode to measure the low-level communication parameters (i.e., RSSI and SNR) for each received frame. To ensure statistical validity, we compute the average results from 1000 frame transmissions.

A. Over-the-Cable Experiments

In the over-the-cable experiment, we mimic perfect channel condition (i.e., flat channel) by connecting USRP and LoRa devices using a coax cable with 30 dB attenuator. The USRP generates a real and emulated (i.e., WiFi frames) LoRa signal. In both cases, the signal is over-sampled with 22 MHz rate. As the LoRa device receives a signal with high power (i.e., reported RSSI at around -25 dBm), the signal degradation (i.e., lower SNR) is attributed to the signal emulation.

Fig. 8 shows spectrograms of the real and the emulated LoRa frames as well as their spectrum profiles. The real 1.625 MHz LoRa signal is clearly visible, while its emulated version can be recognized around the center frequency. However, the latter signal contains a noise caused by additional

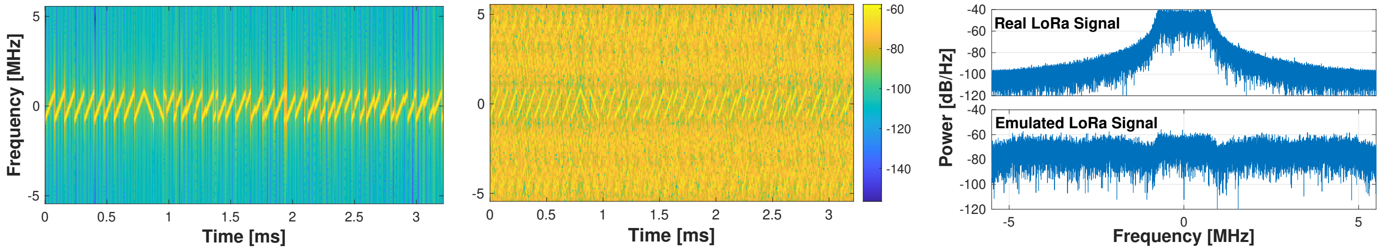

Fig. 8: Spectogram of real (left) and emulated (middle) LoRa frames as well as their spectrum profiles (right).

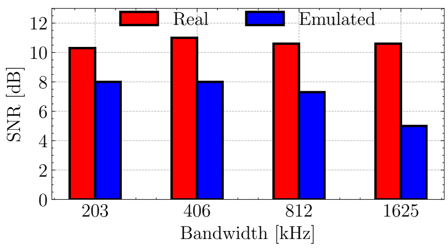

Fig. 9: Comparison of SNR of real and emulated LoRa signals.

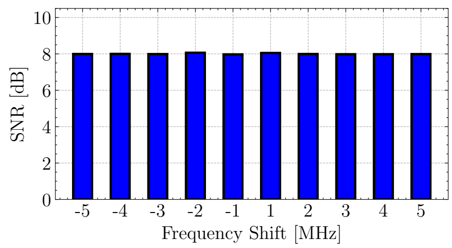

Fig. 10: SNR of an emulated LoRa signal shifted within the BW of a WiFi frame.

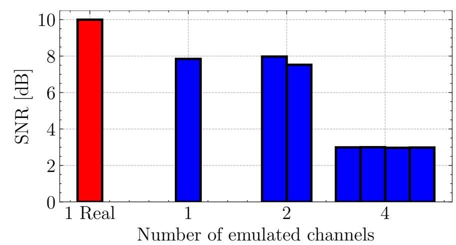

Fig. 11: SNR of multiple LoRa channels emulated in a single WiFi frame.

frequency components introduced by the CCK modulator. The resulting power loss (around 20 dB) can be partially compensated as the TX power of 2.4 GHz LoRa is limited to 8 dBm, while the limit for 802.11b CCK is 18 dBm.

Fig. 9 compares `Wi-Lo` and the real LoRa performance with respect to the reported SNR value at the LoRa receiver side. Although the TX power is the same in both cases, the SNR differs. In general, the larger the bandwidth, the SNR drop is higher. For example, in the case of $SF = 5$, the SNR drop equals 2.3 dB when $BW = 203\,kHz$ and 5.5 dB for $BW = 1625\,kHz$. Such behavior is expected, as with wider bandwidth, the averaging effect of the LPF in the LoRa receiver is weaker, i.e., the waveform imperfections due to signal emulation are not smoothed out. We observed a similar or lower SNR drop for higher values of SF. In practice, the SNR drop plays a minor role as the required SNR for LoRa is very low, i.e., -2.5 dB and -20 dB for $SF = 5$ and $SF = 12$, respectively. Note that in all experiments, the frame error rate was very close to 100%, hence, we do not show this metric.

B. Emulation of Multi-Channel LoRa Transmissions

To verify the multi-channel emulation feature of `Wi-Lo`, we again test the performance of emulated LoRa signal in terms of the SNR drop. Again, we transmit the signal over coax cable so the degradation is attributed entirely to the emulation. For LoRa transmission, we use $SF = 5$ and $BW = 406\,kHz$. Fig. 10 shows SNR as reported by the LoRa receiver when emulating a single LoRa transmission centred at different frequencies within the WiFi bandwidth. Specifically, the LoRa waveform was shifted in frequency by an integer multiple of 1 MHz. The LoRa receiver was tuned to the correct frequency. In all cases, the measured SNR equals around 8 dB, which shows that the approach is feasible.

Fig. 11 shows the reported SNR values, when emulating multiple LoRa transmissions separated by 2 MHz in a single WiFi frame. As we can observe, the SNR drops with the number of simultaneous LoRa transmissions. The effect can be again explained by imperfect signal emulation. Specifically, given the limited codeword set, it is much harder to find a codeword approximating multiple transmissions simultaneously, hence, each individual LoRa signal is more degraded.

C. Over-the-Air Experiment

During the over-the-air experiment, we used commodity Intel NUC mini-PC with WiFi card as `Wi-Lo` transmitter as well as a real LoRa transmitter. Both were placed indoors and configured to periodically (i.e., every 1s) send (emulated and real) LoRa frames with a bandwidth of $BW = 1625\,kHz$, $SF = 6$ and code rate 4/5. The LoRa receiver was mobile, i.e., we carried it indoors and outdoors within a radius of 250 m around the transmitter. For each received frame the RSSI and the SNR as reported by LoRa chip was collected — Fig. 12. As in the previous wired experiment, we see SNR degradation due to emulation. However, the reduction in SNR is not a problem in real setups as the long-range signal reception is mostly limited by the sensitivity of LoRa receiver. Specifically, the lowest RSSI for which LoRa packets were correctly received was -103 dBm, which was the same for both baseline and `Wi-Lo`. In the region of very weak signal levels, we see almost no difference in the SNR of both real LoRa and `Wi-Lo`.

D. Distance Measurements

Finally, we performed outdoor experiments on the university campus to find out the maximum communication distance of `Wi-Lo`. We used the same setup as in the previous experiment but placed it at the window board next to an opened window (10 m above the ground). We used LoRa and WiFi devices operating in the sniffer and monitor mode, respectively. Note that both were receiving the same frame WiFi frame, but the latter decodes it as a LoRa signal. During the measurements,

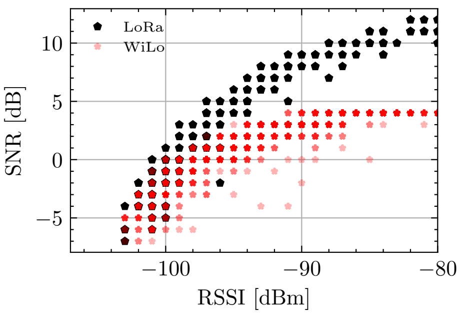

Fig. 12: Comparison of RSSI and SNR of real and emulated LoRa signals in an over-the-air experiment ($SF = 6$).

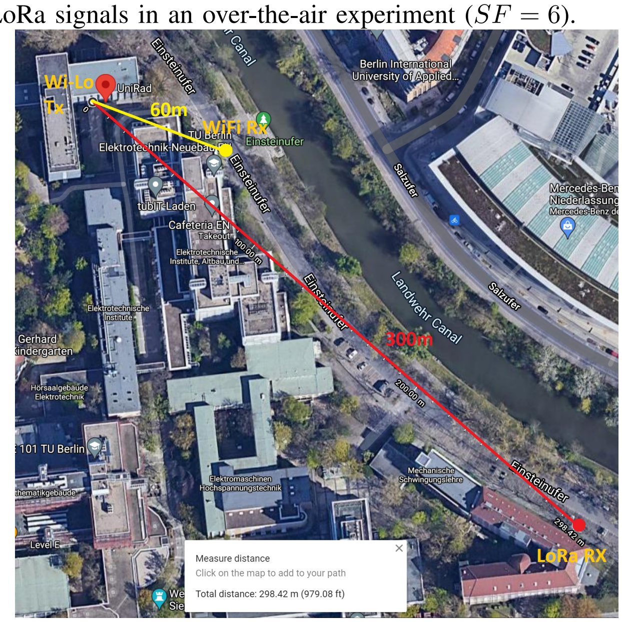

Fig. 13: Long-distance measurements.

we walked away from the transmitter. The propagation characteristic was non-line-of-sight (NLOS) as large buildings were blocking the LOS path. Fig. 13 shows the maximum distance at which the receiver was able to reliably receive frames, i.e., 60 m for WiFi and around 300 m for LoRa. Note that using Wi-Lo the same signal generated by a WiFi device can be correctly received at $5\times$ longer distance when decoded as LoRa waveform. Therefore, Wi-Lo brings an interesting opportunity of trading data rate for communication distance.

V. Related Work

The signal emulation technique was introduced in a pioneering CTC scheme called WeBee [11], which enabled a WiFi device to transmit (i.e., emulate) a ZigBee signal by proper selection of its frame payload bits. It operated with the native data rates of ZigBee but suffered from a high packet error rate due to the inherent distortions of the emulated signal. TwinBee [12], LongBee [13], and WIDE [14] further improve the quality of signal emulation and hence reliability of WEBee. Then, the signal emulation enabled CTC between WiFi and Bluetooth [15], WiFi and LTE [16]. Since these schemes rely on the OFDM modulator of 802.11n WiFi, they cannot perfectly emulate foreign waveform during cyclic prefix (i.e., an inherent feature of OFDM), which constitutes 20% of each symbol time. Here, we show that the CCK-based modulator of 802.11b WiFi can be used as a PWM generator, that can generate a valid LoRa waveform. Li *et al.* [17] showed that with CCK-based signal leaves some unique signatures when it flows into the BLE receiver. The authors proposed a technique called symbol transition mapping to convey data between WiFi and BLE. The reverse direction, i.e., from LoRa to WiFi, can be realized with XFi [6] scheme, that uses the so-called signal hitchhiking technique, i.e., when a smartphone is receiving a WiFi packet from an AP, IoT devices transmit simultaneously, leading to intentional collisions with the WiFi packet in the air. This way, the LoRa data hitchhikes on the WiFi packet and enters the WiFi radio, where it is decoded through waveform reconstruction and subsequent LoRa decoding.

VI. Conclusion

We propose Wi-Lo, a signal emulation technique that enables a WiFi device to transmit valid LoRa frames. It is based on 802.11b CCK modulation, which is available even in the newest WiFi devices due to backward compatibility. Our evaluation with a COTS-based prototype demonstrates that Wi-Lo generates reliable LoRa transmissions with only a small loss in the signal SNR value.

References

[1] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O.Hersent, "LoRaWAN Specification," LoRa Alliance, Standard V1.0, 1 2015. [Online]. Available: https://lora-alliance.org/resource_hub/lorawan-specification-v1-0/

[2] F. R. Andersen, K. D. Ballal, M. N. Petersen, and S. Ruepp, "Ranging Capabilities of LoRa 2.4 GHz," in *IEEE WF-IoT*, 2020.

[3] J. Shi, X. Chen, and M. Sha, "Enabling Direct Messaging from LoRa to ZigBee in the 2.4 GHz Band for Industrial Wireless Networks," in *IEEE ICII*, 2019.

[4] Z. Li and Y. Chen, "Achieving Universal Low-Power Wide-Area Networks on Existing Wireless Devices," in *IEEE ICNP*, 2019.

[5] ——, "BLE2LoRa: Cross-Technology Communication from Bluetooth to LoRa via Chirp Emulation," in *IEEE SECON*, 2020.

[6] R. Liu, Z. Yin, W. Jiang, and T. He, "XFi: Cross-technology IoT Data Collection via Commodity WiFi," in *IEEE ICNP*, 2020.

[7] IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE, Std 802.11-2012, Mar. 2012.

[8] N. Seller and O. B. Sornin, "Low Power Long Range Transmitter," US Patent Office, US Patent 9,252,834, Feb. 2016.

[9] J. Haxhibeqiri, E. D. Poorter, I. Moerman, and J. Hoebeke, "A Survey of LoRaWAN for IoT: From Technology to Application," *MDPI Sensors*, 2018.

[10] Semtech, "Physical Layer Proposal: 2.4GHz ISM Band," https://lora-developers.semtech.com/documentation/tech-papers-and-guides/physical-layer-proposal-2.4ghz/, 2021, [Online; accessed 26-Oct-2021].

[11] Z. Li and T. He, "WEBee: Physical-Layer Cross-Technology Communication via Emulation," in *ACM MobiCom*, 2017.

[12] Y. Chen, Z. Li, and T. He, "TwinBee: Reliable Physical-Layer Cross-Technology Communication with Symbol-Level Coding," in *IEEE INFOCOM*, 2018.

[13] Z. Li and T. He, "LongBee: Enabling Long-Range Cross-Technology Communication," in *IEEE INFOCOM*, 2018.

[14] X. Guo, Y. He, J. Zhang, and H. Jiang, "WIDE: Physical-level CTC via Digital Emulation," in *ACM/IEEE IPSN*, 2019.

[15] W. Jiang, Z. Yin, R. Liu, Z. Li, S. M. Kim, and T. He, "BlueBee: A 10,000x Faster Cross-Technology Communication via PHY Emulation," in *ACM SenSys*, 2017.

[16] P. Gawłowicz, A. Zubow, S. Bayhan, and A. Wolisz, "Punched Cards over the Air: Cross-Technology Communication Between LTE-U/LAA and WiFi," in *IEEE WoWMoM*, 2020.

[17] L. Li, Y. Chen, and Z. Li, "WiBle: Physical-Layer Cross-Technology Communication with Symbol Transition Mapping," in *IEEE SECON*, 2021.