# LoPhy: A Resilient and Fast Covert Channel over LoRa PHY

Boya Liu
Zhejiang University
Hangzhou, China
boyal@zju.edu.cn

Chaojie Gu
Zhejiang University
Hangzhou, China
gucj@zju.edu.cn

Shibo He
Zhejiang University
Hangzhou, China
s18he@zju.edu.cn

Jiming Chen
Zhejiang University
Hangzhou, China
cjm@zju.edu.cn

## ABSTRACT

Covert channel, which can break the logical protections of the computer system and leak confidential or sensitive information, has long been considered a security issue in the network research community. However, recent research has shown that cooperative agents can use the "covert" channel to augment the communication of legitimate applications, rather than by adversaries seeking to compromise computer security. This further broadens the potential applications of covert channels. Despite this, the design and implementation of covert channels in the context of Low Power Wide Area Networks (LPWANs) have not been widely discussed. Current state-of-the-art uses On-off keying (OOK) on LoRa PHY to create a covert channel, but this channel has limited transmission distance and capacity. In this paper, we propose LoPhy, a resilient and fast covert channel over LoRa physical layer (PHY). LoPhy uses the Chirp Spreading Spectrum (CSS) modulation scheme to increase its resilience and explore the trade-off between the covert channel's capacity and the legitimate channel's resilience. We implement the proposed covert channel on off-the-shelf devices and software-defined radios and show that LoPhy achieves a 0.57% bit error rate at a distance of 700 m without affecting the legitimate channel's performance. Moreover, we present two applications enabled by LoPhy to demonstrate the potential of LoPhy. Compared with the state-of-the-art, LoPhy brings up to 18× reduction of bit errors and 63× gain on noise resilience.

## CCS CONCEPTS

• **Computer systems organization** → **Embedded and cyber-physical systems**; • **Hardware** → **Wireless devices**; **Digital signal processing**; • **Networks** → *Physical links*; *Network protocol design.*

## KEYWORDS

Covert communication, LoRa

*IPSN '23, May 09–12, 2023, San Antonio, TX, USA*

ACM ISBN 979-8-4007-0118-4/23/05…$15.00
https://doi.org/10.1145/3583120.3586952

**ACM Reference Format:**
Boya Liu, Chaojie Gu, Shibo He, and Jiming Chen. 2023. LoPhy: A Resilient and Fast Covert Channel over LoRa PHY. In *The 22nd International Conference on Information Processing in Sensor Networks (IPSN '23), May 09–12, 2023, San Antonio, TX, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3583120.3586952

## 1 INTRODUCTION

Recent decades have witnessed the prosperous development of Internet-of-things (IoT) in many areas, including public services, smart cities, smart agriculture, industrial manufacturing, etc. Low Power Wide Area Network (LPWAN), an emerging wireless IoT technology that supports long-distance communication up to several kilometers, significantly increases the connectivity and efficiency of IoT. Among existing LPWAN technologies (including NB-IoT [45], SigFox [8], and Weightless-P [52]), LoRaWAN [2] stands out due to its open data link standard, use of license-free Industrial Scientific Medical (ISM) bands, and the independence from managed infrastructures provided by Internet Service Provider (ISP).

In past years, tremendous efforts have been devoted to improving the performance of LoRaWAN and its physical layer standard LoRa, including communication range extension [35], multiple access mechanisms [17], and collision resolving [10, 36, 58]. Additionally, many innovative applications based on LoRa/LoRaWAN have been developed, including target localization and tracking [5, 22, 30, 39], long-range sensing [59, 62], and aggregate queries retrieving [16]. Except for the aforementioned studies on performance improvement and pilot application development, the security of LoRa/LoRaWAN also is a critical research problem. Despite the common threats that computer communication faces (e.g., jamming and replay attack [3], impersonating attack [41], key compromising attack [9]), the covert channel attack has been merely discussed. The LoRaWAN security mechanism protects the upper layer except for the physical layer, i.e., LoRa, which makes LoRa vulnerable to the covert channel attack [29]. The covert channel is defined as a channel that is not intended for information transfer but can leak sensitive information [33]. The state-of-the-art covert channel over LoRa is CloakLoRa [29], which employs On-Off Keying (OOK) to modulate information on the amplitude of LoRa. However, CloakLoRa has a limited communication range because OOK is known as not resilient to noise [29]. Moreover, CloakLoRa attenuates the transmission power to create different symbols. The power restriction on the ISM band [13], along with the power attenuation limits the communication range of CloakLoRa. CloakLoRa achieves a 250 m communication range.

In this paper, we present LoPhy (LPWAN over LoRa PHY), a resilient and fast covert channel over LoRa physical layer (PHY). This work is primarily motivated by scenarios where the "covert" channel is used by cooperative agents to augment the communication of legitimate applications, as opposed to being used by an adversary. The long-range communication capability of LoRa is enabled by Chirp Spread Spectrum (CSS) modulation. As a spread spectrum modulation technique, CSS uses its entire allocated bandwidth to broadcast a signal, making it robust to channel noise and resistant to multi-path fading [38]. Similarly, we revisit the design covert channel over LoRa PHY with CSS to boost the communication range. LoPhy modulates covert information as chirps into the amplitude of LoRa signals. Moreover, unlike the networking technologies used for legitimate channels, LoPhy does not have to follow standards to regulate its parameters and thus has a larger feasible space for parameter selection. Compared with LoRa, LoPhy supports a smaller spreading factor (e.g., 3, 4, 5), which enables fast data transmission due to the nature of CSS. The spreading factor used in the proposed covert channel does not need to follow the regulation in LoRa/LoRaWAN standards. Further, we demonstrate how LoPhy enables two new applications, i.e., channel aggregation and data timestamping, which help improve the throughput and save energy of the legitimate channel.

The design of LoPhy is challenging due to three practical issues. The first challenge is the absence of the imaginary part in the LoPhy chirp. CSS performs de-chirping, a signal processing technique, on the received chirp to converge the energy spreading over the entire bandwidth to get signal-to-noise ratio (SNR) gain. The input variables required by the de-chirping operation are complex values. However, as LoPhy modulates the LoRa signal's amplitude that is a real value, its chirp cannot be de-chirped and thus achieves SNR gain. Since the LoPhy's carrier signal, i.e., LoRa, is a double-sideband (DSB) signal, we cannot apply the Hilbert transform to obtain the imaginary part like single-sideband (SSB) signals, e.g., sound. To enable de-chirping in LoPhy, we propose an imaginary part generation method based on detailed analysis, which enables de-chirping for LoPhy chirps and gains noise resilience. The second challenge is quantifying the impact of the power adjustment on the covert channel. LoPhy embeds its chirps by adjusting the transmission power of the end device, which may affect the performance of the covert channel and break the transmission power restriction on ISM bands. To suppress side effects on the covert channel caused by power adjustment, we discuss the possible power adjustment approaches and analyze their impacts, which guide the covert channel configuration. Another challenge is the compatibility with commercial off-the-shelf (COTS) LoRa end devices. It is impossible for a COTS LoRa end device to adjust its instantaneous power. LoPhy tackles this challenge with a specifically designed approximate chirp synthesization using a radio frequency programmed attenuator.

We implement the prototype of LoPhy transmitter and receiver. LoPhy adds a radio frequency programmed attenuator to a COTS LoRa end device as the transmitter. We use a low-cost receive-only SDR dongle (i.e., RTL-SDR) to receive the covert signal. We conduct extensive indoor and outdoor experiments (up to 1 km) to evaluate the performance in various settings. Our result shows that our prototype can build a super resilient covert channel with low bit error rates when the transmitter and receiver are separated up to 900 m. Meanwhile, the communication of the covert channel does not affect that of the legitimate channel. Besides, we also conduct experiments and simulations to compare LoPhy with the state-of-the-art system, i.e., CloakLoRa. Experimental results show that LoPhy and CloakLoRa achieve 1.917% BER and 36.694% BER at the distance of 500 m, respectively. Simulational results indicate that LoPhy brings 63× gain on noise resilience with respect to CloakLoRa. In addition, we also explore the maximum bandwidth and data rate of LoPhy with extensive simulations in various parameter settings and channel conditions. The simulational results show that the bandwidth of LoPhy can reach 250 kHz on average and the bit rate is the same order of magnitude as the legitimate channel.

In summary, our work makes three major contributions:

- We study a new covert channel LoPhy over LoRa physical layer which is super resilient to noise and compatible with the legitimate LoRa channel.
- We implement the LoPhy on COTS devices and conduct extensive experiments and simulations to evaluate its performance. Compared with the state-of-the-art (i.e., CloakLoRa), LoPhy is more resilient to noise (63×) at the same throughput (200 bps).
- We present two new applications enabled by LoPhy, which help improve the throughput and save energy of the legitimate channel.

The rest of this paper is organized as follows. §2 introduces the primer of modulation, demodulation, and frame structure in LoRa. §3 provides an overview of LoPhy and challenges. §4 presents the design of LoPhy. §5 presents a detailed analysis and implementation of LoPhy. §6 presents the experimental and simulational results under different conditions. §7 studies the potential applications of LoPhy. §8 reviews related work. §9 discusses several issues. Finally, §10 concludes this paper.

## 2 LORA PRIMER

LoRa adopts Chirp Spread Spectrum (CSS) scheme at its PHY. In this section, we will introduce the preliminary knowledge of CSS modulation, demodulation, and LoRa frame structure.

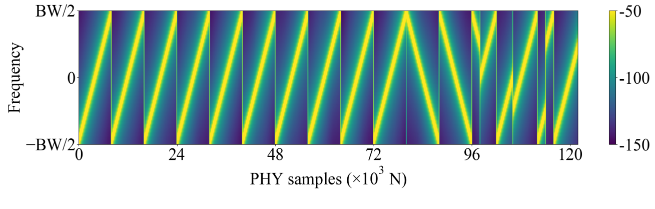


**Figure 1: The spectrogram of a typical LoRa frame.**

**Modulation.** In CSS modulation, the signal is modulated as chirps. Each chirp sweeps a specified bandwidth $BW$ linearly with time during its symbol time $T_s$. An up-chirp starting from its initial

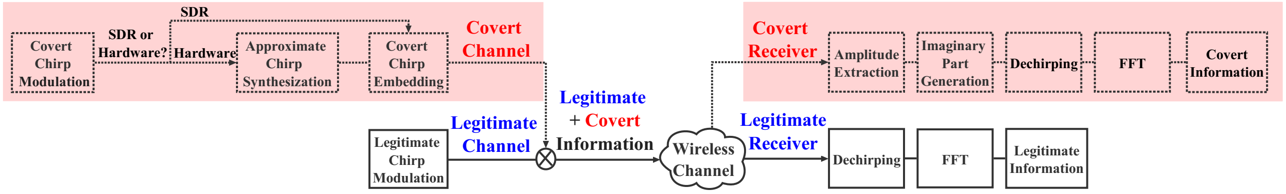


**Figure 2: LoPhy: a resilient and fast covert channel over LoRa PHY.**

frequency linearly increases in frequency over time, reaches the maximum frequency $f_{max}$, wraps around, and continues sweeping from the minimum frequency $f_{min}$ back to its initial frequency, while a down-chirp is the opposite. A base up-chirp, denoted by $C_0(t)$, whose frequency increases from $-\frac{BW}{2}$ to $\frac{BW}{2}$, can be mathematically expressed by

$$f(t) = f_0 + k \cdot t = -\frac{BW}{2} + \frac{BW}{T_s} t; 0 \le t \le T_s; T_s = \frac{2^{SF}}{BW},$$
$$C_0(t) = e^{j \int 2\pi f(t) dt} = e^{j2\pi t(-\frac{BW}{2} + \frac{BW}{2T_s} t)}, \qquad (1)$$

where $SF$ is the spreading factor. Given an $SF$, CSS uses different initial frequencies of chirps to represent different $SF$-bit symbols. To achieve this, CSS evenly divides the $BW$ into $2^{SF}$ bins as different initial frequencies, denoted by $f_\varphi$, where $\varphi \in \{0, 1, \cdots, 2^{SF} - 1\}$. CSS shifts the initial frequency of the base up-chirp (Eq. 1) to $f_\varphi$ to represent different symbols. Thus, an up-chirp whose initial frequency is $f_\varphi$ and amplitude is $A(t)$ can be denoted as

$$C_\varphi(t) = A(t) \cdot C_0(t) \cdot e^{j2\pi f_\varphi t}. \qquad (2)$$

**Demodulation.** A received chirp can be denoted as $C'_\varphi(t) = C_\varphi(t) + n(t)$, where $n(t)$ is noise. To retrieve the encoded data, the receiver estimates the initial frequency $f_\varphi$ of the chirp. Specifically, as shown in Eq. 3, the receiver first performs a de-chirping process by multiplying the received chirp with a local-generated base down-chirp, denoted by $C_0{}^*(t)$,

$$C'_\varphi(t) \cdot C_0{}^*(t) = A(t) \cdot e^{j2\pi f_\varphi t} + n(t) C_0{}^*(t). \qquad (3)$$

After de-chirping, the received signal is transformed to a sinusoid of constant frequency $f_\varphi$ which is exactly the initial frequency of the chirp $C_\varphi$. Thus, the receiver recovers the frequency $f_\varphi$ by locating the peak of a $2^{SF}$ points FFT of the de-chirped signal in Eq. 3, which can be expressed by

$$\varphi\left[C'_\varphi(t)\right] = \arg\max\left\{FFT\left[C'_\varphi(t) \cdot C_0{}^*(t)\right]\right\}, \qquad (4)$$

where $\varphi[C'_\varphi(t)]$ represents the peak location in the FFT result. By comparing energy intensity across all FFT bins, the receiver can detect the FFT peak location and recover $f_\varphi$. In contrast, since the frequency of base down-chirp $C_0{}^*(t)$ varies with time, the energy of the second part in Eq. 3 spreading over the whole bandwidth after de-chirping, leading to a low energy intensity. As a result, de-chirping helps the received signal converge its energy and achieve SNR gain.

**LoRa frame.** Fig. 1 presents the spectrogram of a typical LoRa frame, which consists of four parts: a *preamble* of 8 base up-chirps (by default), a *sync word* of 2 up-chirps, a *Start Frame Delimiter (SFD)* of 2.25 base down-chirps, and a *payload* of multiple data chirps.

## 3 LOPHY OVERVIEW

In this section, we provide an overview of LoPhy and challenges. LoPhy aims to build a resilient covert channel over LoRa PHY while not affecting legitimate channel communication. Fig. 2 presents the system architecture of LoPhy. In the transmitter, the covert chirp is modulated and embedded into the modulated legitimate chirp. After receiving the signal, the legitimate receiver does not inspect the amplitude information and performs demodulation as usual. The covert receiver requires two additional steps, i.e., amplitude extraction and imaginary part generation, before applying the standard demodulation approach.

To achieve such a design, we address the following challenges. (1) ***Generating the absent imaginary part:*** LoPhy generates the imaginary part of the received signal, which is unavailable because the amplitude is a real value. With the generated imaginary part, the SNR of the received LoPhy chirp can be further boosted by de-chirping. (2) ***Understanding the impact of power adjustment:*** LoPhy modulates covert chirps into the amplitude of the LoRa frame by adjusting the transmission power of the end node. LoPhy selects its power adjustment schemes according to regulations on ISM bands. (3) ***Accommodating* LoPhy *to COTS devices:*** To implement LoPhy using COTS LoRa end devices, LoPhy modulates the chirp by approximating a sequence of discrete frequency levels using a radio frequency programmed attenuator.

## 4 DESIGN OF LOPHY

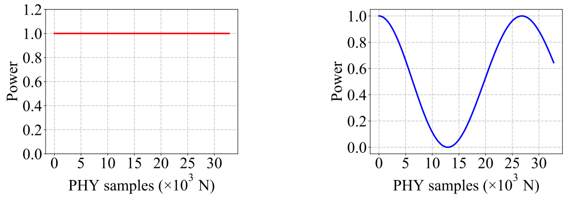
In this section, we describe the design of LoPhy, including modulation (§4.1), demodulation (§4.2), and fine tuning for packet detection and reception (§4.3).

### 4.1 Modulation of Covert Channel

**Covert chirp modulation.** LoPhy aims to embed the covert information in LoRa PHY. LoPhy adopts CSS modulation to enhance the noise resilience of the covert channel. Ideally, chirps of the covert channel can be formulated as

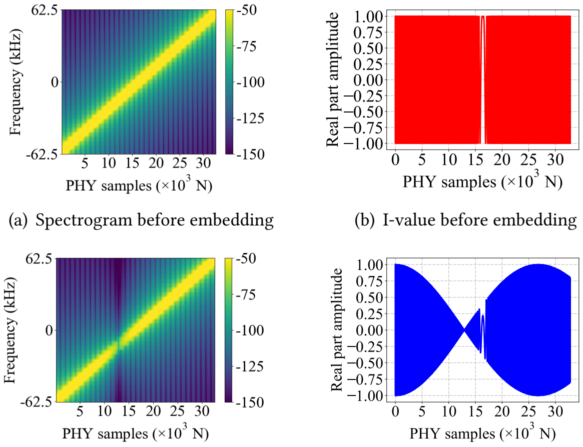
$$\begin{aligned} &C_{0_c}(t) = e^{j\int 2\pi f_c(t) dt}, \\ &C_{\varphi_c}(t) = A_c(t) \cdot C_{0c}(t) \cdot e^{j2\pi f_{\varphi_c} t}, \\ &R_{\varphi_c}(t) = \mathrm{Re}\left[C_{\varphi_c}(t)\right], \\ &0 \le t \le T_{s_c}, T_{s_c} = \frac{2^{SF_c}}{BW_c}, \end{aligned} \qquad (5)$$

where $C_{0_c}(t)$ and $C_{\varphi_c}(t)$ are base up-chirp (Eq. 1) and data chirp (Eq. 2), respectively. Similar to the legitimate channel, the covert channel has its own bandwidth $BW_c$ and spreading factor $SF_c$. Thus, $\varphi_c \in \{0, 1, \cdots, 2^{SF_c} - 1\}$. Note that LoPhy works on LoRa PHY by embedding the covert information into the amplitude of the power level of the legitimate channel, it cannot adopt a "full" CSS modulation due to the imaginary part of the chirp being unavailable.



(a) Power before embedding (b) Power after embedding

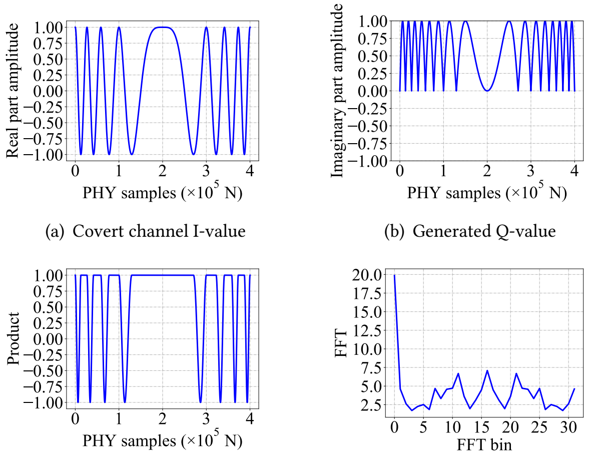
**Figure 3: Comparison of power level of a LoRa chirp (SF = 12, BW = 125 kHz) before and after embedding.**



(a) Spectrogram before embedding (b) I-value before embedding

(c) Spectrogram after embedding (d) I-value after embedding

**Figure 4: Comparison of the spectrogram, I-value of a LoRa chirp (SF = 12, BW = 125 kHz) before and after covert channel embedding.**



(a) Covert channel I-value (b) Generated Q-value

(c) Covert channel de-chirping (d) Covert channel FFT

**Figure 5: Demodulation process of the covert channel.**

As a result, in practice, we can only get the real part of the covert chirp, which is denoted by $R_{\varphi_c}(t)$ in Eq. 5.

**Covert chirp embedding.** To embed the covert chirps, LoPhy modulates the amplitude of the power level of LoRa chirps with CSS. Note that such an amplitude modulation is performed on channels where frequency modulation has already been completed. Thus, the covert channel embedding does not affect the initial frequency of the legitimate LoRa chirp because it is a process of scaling each sample point. When the covert channel has a high bandwidth, it may introduce new frequency components. However, the de-chirping procedure can converge the spectrum power of a chirp to a certain frequency point, which is much greater than the power of the introduced frequency components. In the following sections, we denote chirps in the covert channel and the legitimate channel as covert chirp (of LoPhy) and legitimate chirp (of LoRa), respectively.

Fig. 3(a) presents the amplitude of the power level of a legitimate chirp. For simplicity, denote the amplitude of the power level as amplitude in the following sections. Ideally, the amplitude of the legitimate chirp, denoted by $A(t)$, remains unchanged over its symbol time. Note that the amplitude of a signal is not a complex value. Thus, to embed the covert chirp in the amplitude, we use the real part of the covert chirp (i.e., I-value) to replace the original $A(t)$ of the legitimate chirp. After embedding, the legitimate chirp with covert information can be represented as

$$R_{\varphi_c}(t) \cdot C_0(t) \cdot e^{j2\pi f_\varphi t}. \tag{6}$$

Fig. 3(b) shows the chirp amplitude after embedding. The amplitude changes over time and the shape of the waveform is the beginning part of the I-value of the covert chirp. Fig. 4 compares the chirp before and after embedding by showing the spectrogram and I-value. Compared with Fig. 4(a), Fig. 4(c) presents explicitly darker samples between 10-15($\times 10^3$), which corresponds to the lower power level of samples between 10-15($\times 10^3$) in Fig. 3(b). Fig. 4(d) also has lower absolute values at the same positions compared with Fig. 4(b). These figures show the signal after embedding from different aspects.

## 4.2 Demodulation of Covert Channel

The right part of Fig. 2 summarizes the covert channel demodulation process. Compared with the demodulation process of the legitimate channel, the covert channel requires two additional steps, i.e., amplitude extraction and imaginary part generation. Note that the real part of the covert chirp signal is already on the baseband. Thus, we do not need to perform extra signal processing to achieve down-conversion.

**Amplitude extraction.** For the legitimate receiver, it will not inspect the amplitude of the packet because it is a standard end device. Differently, the covert receiver inspects the amplitude information as shown in Fig. 5(a). Specifically, the amplitude of the received LoRa frame is computed by

$$A(t) = I(t)^2 + Q(t)^2, \tag{7}$$

where $I(t)$ and $Q(t)$ are the in-phase and quadrature values captured by covert receivers.

**Imaginary part generation.** Recall that the covert chirp is embedded into the amplitude, which is a real value. However, in CSS modulation, the receiver needs both the real part and the imaginary part to converge the spectrum power of a chirp to a certain frequency point. To achieve such an SNR gain, the receiver needs to generate the corresponding imaginary part according to the real part. However, as LoPhy leverages LoRa as the carrier

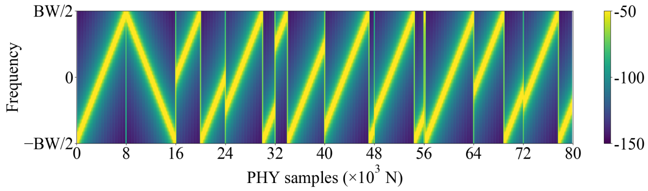


**Figure 6: The frame structure of LoPhy.**

wave, which is a DSB signal, we cannot directly apply the Hilbert transform to get the imaginary part. This is because the Hilbert transform introduces different phase shifts for different frequency parts of the DSB signal, i.e., 90° for the upper sideband and −90° for the lower sideband, which would not generate the imaginary part of the signal as expected. To this end, we propose an imaginary part generation method as follows.

In CSS modulation, the real part and the imaginary part of a chirp share the same phase, as shown in Eq. 8. Thus, we can perform an *arccos* operation to the real part to calculate the shared phase and then perform a *sin* operation to get the corresponding imaginary part. Though the quadrant information of the phase is lost, the frequency information is preserved, which is enough for accurate demodulation. We will analyze this issue in §5.1. Fig. 5(b) shows a locally generated imaginary part.

$$\begin{aligned} &\cos\varphi + \sin\varphi \cdot j = C, \\ &I_{\varphi_c}(t) = \sin\left\{\arccos\left[R_{\varphi_c}(t)\right]\right\}. \end{aligned} \tag{8}$$

After we have the imaginary part, we can use the local-generated covert base down-chirp to perform the de-chirping and retrieve the covert information. Fig. 5(c) and Fig. 5(d) present the de-chirping result and FFT result, respectively. Fig. 5(d) shows the frequency domain representation of the product in the time domain (Fig. 5(c)), with a corresponding peak on the first FFT bin (index 0).

## 4.3 Covert Channel Fine Tuning

**LoPhy framing.** As shown in Fig. 6, a LoPhy frame consists of two parts, a *sync word* of a base covert up-chirp and a base covert down-chirp, a *payload* of multiple data chirps. Note that we cannot distinguish the covert up-chirp and the covert down-chirp according to their real parts, which are the same. Thus, the unique pattern of *sync word* is set to be a covert up-chirp and the opposite number of a covert down-chirp. The LoPhy frame does not contain a *preamble* because LoPhy modulates the amplitude of the legitimate channel, which means the receiver does not need to utilize *preamble* to correct the carrier frequency offset (CFO) [56]. In LoPhy, the covert chirp modulation is started from the beginning of the LoRa frame.

**Frame detection.** To detect the LoPhy frame, the receiver uses a two-step approach: (1) *Legitimate LoRa frame detection:* As shown in Fig. 1, the last up-chirp of the *sync word* and the first down-chirp of the *SFD* exhibit a unique "peak" pattern, which can be taken as a template. At run time, the receiver performs cross-correlation on the received signal and locates the LoRa frame. Note that the LoRa frame detection can be implemented in multiple ways, including folding [21], Schmidl-Cox algorithm [47], and deep learning [22]. (2) *Covert* LoPhy *frame detection:* We can use a similar approach in the standard LoRa for detection. As shown in Fig. 6, the *sync word* in the LoPhy frame exhibits a unique pattern. However, as mentioned in §4.1, the covert chirp which only has real parts is different from the regular chirp, which means that the receiver cannot distinguish between the covert up-chirp and the covert down-chirp. Thus, we use a covert up-chirp and the opposite number of covert down-chirp as the template for correlation. With this prior knowledge, the receiver locally generates the template and performs cross-correlation with the received signal. Additionally, we can leverage GPU to accelerate the frame detection process [22].

# 5 ANALYSIS AND IMPLEMENTATION

In this section, we provide a detailed analysis of LoPhy to answer the following questions.

- **Q1 (§5.1)**: *How much information is lost during the imaginary part generation process?*
- **Q2 (§5.2)**: *How does power adjustment caused by the covert channel embedding affect the performance?*
- **Q3 (§5.3)**: *How to apply LoPhy for COTS LoRa end devices?*

## 5.1 Impact of Information Loss

Since the amplitude is a real value, LoPhy embeds and transmits the real part of the covert chirp and discards the imaginary part. The imaginary part needs to be generated locally at the receiver side to enable de-chirping in the covert channel. Fig. 7(a) compares the original imaginary part and the generated one. The generated imaginary part retains the positive part corresponding to the original signal but modifies the negative part to its opposite number. As shown in Eq. 8, mathematically, *arccos* is a multivalued function and is ruled to choose the value in $[0, \pi]$. Therefore, the quadrant information of the phase $\varphi$ is lost. In this section, we theoretically and experimentally analyze the information loss in the imaginary part generation. The analysis results help us better understand the rationale behind LoPhy and assist optimal parameter configuration for LoPhy.

**Analysis.** To understand the impact of the information loss due to imaginary part generation, we mathematically deduce demodulation processes of a standard up-chirp (denoted by $C_{\varphi_c}$) and an up-chirp with a local-generated imaginary part (denoted by $\hat{C}_{\varphi_c}$) in the covert channel. The standard up-chirps (Eq. 5) can be transformed to trigonometric representation by Euler's formula to Eq. 9, and the standard down-chirp is also transformed in the same way. For simplicity, parts of the formulas are abbreviated to $\alpha$ and $\beta$, respectively.

$$\begin{aligned} C_{\varphi_c}(t) =& C_{0c}(t) \cdot e^{j2\pi f_{\varphi_c} t} \\ =& \cos 2\pi \underbrace{\left(f_{\varphi_c} - \frac{BW_c}{2} + \frac{{BW_c}^2}{2 \cdot 2^{SF_c}} t\right)}_{\alpha} t + j \cdot sin2\pi\alpha t, \\ {C_{0c}}^*(t) =& e^{j2\pi t(\frac{BW_c}{2} - \frac{{BW_c}^2}{2\cdot 2^{SF_c}} t)} \\ =& \cos 2\pi \underbrace{\left(\frac{BW_c}{2} - \frac{{BW_c}^2}{2 \cdot 2^{SF_c}} t\right)}_{\beta} t + j \cdot sin2\pi\beta t. \end{aligned} \tag{9}$$

Accordingly, the generated imaginary part in Fig. 7(a) can be expressed by the absolute value of the original one. The de-chirping of an up-chirp with a local-generated imaginary part $\hat{C}_{\varphi_c}$ can be expressed by

$$\begin{aligned}&\hat{C}_{\varphi_c}(t)\cdot {C_{0_c}}^*(t)\\ &=[\cos 2\pi\alpha t+j\cdot|\sin 2\pi\alpha t|]\cdot[\cos 2\pi\beta t+j\cdot\sin 2\pi\beta t].\end{aligned}\tag{10}$$

The absolute value sign of $sin(\cdot)$ in $\hat{C}_{\varphi_c}$ affects the product of de-chirping. Let $|\sin 2\pi\alpha t|=0$, we can segment the signal to choose the original value or opposite value to get rid of the absolute value sign as shown in Eq. 11,

$$\begin{aligned}&t_i=2^{SF_c-1}\cdot\frac{1\pm\sqrt{1-2^{2-SF_c}\cdot k}}{BW_c};0\le t\le\frac{2^{SF_c}}{BW_c};k\in Z,\\ &|\sin 2\pi\alpha t|=\left\{\begin{array}{c}-\sin 2\pi\alpha t;t\in t_1\\ \sin 2\pi\alpha t;otherwise\end{array}\right.,\end{aligned}\tag{11}$$

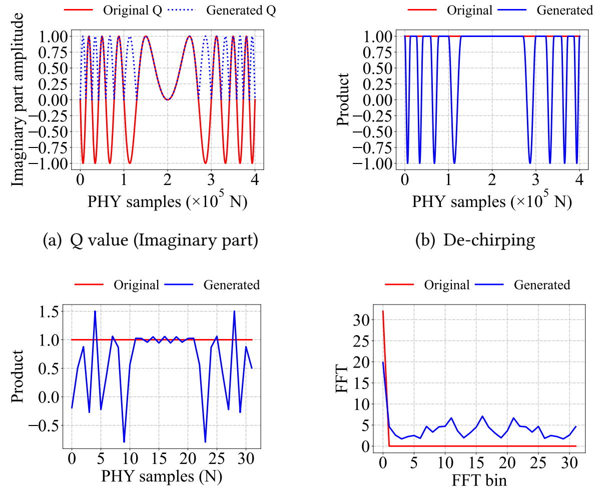
where $t_1$ is just a symbol and the specific value range of $t$ in Eq. 11 is to be confirmed according to the relationship between the original value and the generated value. For example, as Fig. 7(a) shows, for this set of parameters, $k$ is calculated to be $k\in[0,8],k\in Z$ and $t_1\in[t_{2m-1},t_{2m})\cup[t_{2n},t_{2n+1}),m\in[1,4],n\in[5,8]$. After segmentation and sign determination, the part equal to the original value is demodulated and corresponds to the single peak $f_{\varphi_c}$, while the part equal to the opposite value is demodulated differently as follows

$$\begin{aligned}&\hat{C}_{\varphi_c}(t)\cdot {C_{0_c}}^*(t)\\ &=[\cos 2\pi\alpha t-j\cdot\sin 2\pi\alpha t]\cdot[\cos 2\pi\beta t+j\cdot\sin 2\pi\beta t]\\ &=\cos 2\pi(\beta-\alpha)t+j\cdot\sin 2\pi(\beta-\alpha)t\\ &=e^{j2\pi(\beta-\alpha)t}=e^{j2\pi(BW_c-f_{\varphi_c}-\frac{{BW_c}^2}{2^{SF_c}}t)t}.\end{aligned}\tag{12}$$

The result shows that there are a series of frequency values according to $t$. Due to the variation of $t$, the peaks will be tiny compared to the peak at $f_{\varphi_c}$ [50].

**Simulation.** To intuitively understand the impact of the information loss, we use an example to illustrate. Considering that there is an up-chirp of $f_{\varphi_c}=0$, $SF_c=5$, $BW_c=80$ Hz in the covert channel. Fig. 7(a) presents original and generated Q values of the up-chirp in the covert channel. Fig. 7(b) and Fig. 7(c) compare their de-chirping products before and after decimation, respectively. According to Fourier Transform, the signal shown in Fig. 7(c) can be expressed by a linear combination of trigonometric functions (sines and/or cosines). The $BW_c$ is evenly divided into $2^{SF_c}$ bins as different initial frequencies, denoted by $f_{\varphi_c}$, where $\varphi_c\in\{0,1,\cdots,2^{SF_c}-1\}$. The signal with frequency falling into the corresponding interval is supposed to have a peak in the corresponding FFT bin. For the generated one, the majority of the signal energy is converged on the first FFT bin whose index is 0, and others are distributed to other frequencies. For the original one, the energy of the whole bandwidth is on the first FFT bin whose index is 0. Fig. 7(d) compares the FFT results corresponding to the two different imaginary parts. The FFT peak of the generated one at 0 is lower than the original one but stands out largely compared to other small peaks. Thus, although there is information loss caused by the imaginary part generation, the remaining information is enough for symbol decoding.

We further use two metrics to qualitatively characterize the impact of the information loss, i.e., estimation error and decoding error.



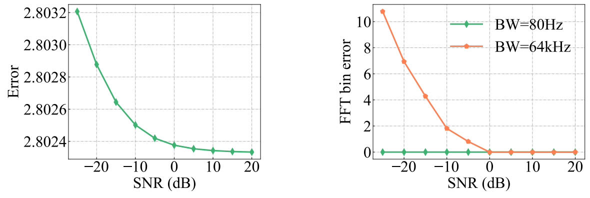
(a) Q value (Imaginary part)

(b) De-chirping

(c) Decimation

(d) FFT

**Figure 7: Intermediate results comparison of demodulating a covert chirp with the original imaginary part and the generated imaginary part.**



(a) Estimation error

(b) Decoding error

**Figure 8: Estimation error and decoding error of the covert chirp.**

The estimation error, denoted by $E_{I,Q}$, is the difference between the original signal and the generated one, which can be expressed by

$$\begin{aligned}E_{I,Q}&=\frac{1}{N}\cdot\int_0^T\left\|\left(R_{\varphi_c}(t)+I_{\varphi_c}(t)\right)-\left(\hat{R}_{\varphi_c}(t)+\hat{I}_{\varphi_c}(t)\right)\right\|_2^2dt\\ &=\frac{1}{N}\cdot\int_0^T\left[\left(R_{\varphi_c}(t)-\hat{R}_{\varphi_c}(t)\right)^2+\left(I_{\varphi_c}(t)-\hat{I}_{\varphi_c}(t)\right)^2\right]dt,\end{aligned}\tag{13}$$

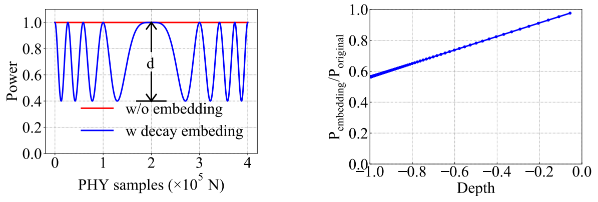
where $R_{\varphi_c}(t), I_{\varphi_c}(t), \hat{R}_{\varphi_c}(t), \hat{I}_{\varphi_c}(t)$ respectively represent the theoretical and estimated real part and imaginary part of a covert chirp, and $N$ represents the PHY samples.

For the decoding error, we calculate the error of the FFT bin location by the difference of the $argmax(\cdot)$ of the FFT ground truth and the estimated FFT, which can be expressed by

$$E_{FFT}=\left\|\arg\max\{FFT\}-\arg\max\left\{\widehat{FFT}\right\}\right\|_1,\tag{14}$$

where $FFT$ and $\widehat{FFT}$ represent the theoretical and estimated value, respectively.

We add Additive White Gaussian Noise (AWGN) on the covert channel to simulate different SNRs scenarios. Fig. 8(a) shows the results of the estimation error when SNR ranges from -25dB to 20dB. The error decreases with better SNR, which means that the estimation of the covert chirp is approaching the ground truth



(a) Decay

(b) Power ratio verse depth in decay

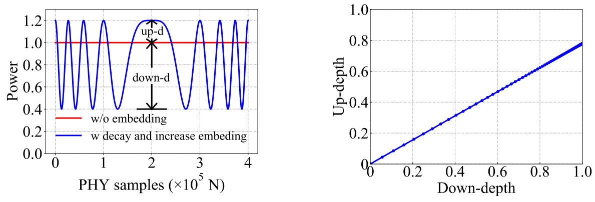
**Figure 9: Modulation depth and power ratio in the case of decay ($SF_c = 5, BW_c = 80Hz$). The maximum power of the waveform with embedding (blue line) is fixed to the original power (red line) and the minimum power can be changed by the right figure.**

gradually. Fig. 8(b) shows the results of the decoding error, which represents the decoding accuracy of the covert channel. When $SF_c = 5, BW_c = 80Hz$, the error remains 0 with SNR ranging from -25dB to 20dB. To illustrate the generality of the variation trend of FFT bin error, we randomly select another set of parameters and plot the results when $SF_c = 5, BW_c = 64kHz$, which shows that with the increase of SNR, the error of the FFT bin decreases. Overall, although the estimation error cannot reach 0 as the existence of channel noise, it does not affect the decoding accuracy which is operating in the frequency domain.

## 5.2 Impact of Power Adjustment

In the process of modulation, LoPhy embeds the real part of the covert chirp into the amplitude of the power level of the legitimate chirp. We can further scale the waveform to have different power ranges (i.e., varying the max and min values of the signal power) to adjust the average power of the covert chirp. Specifically, according to the comparison between instantaneous powers of signals with and without covert channel embedding, there are three cases, i.e., power decay, power increase, and decay and increase combination. In the case of power decay, the instantaneous power and average power after embedding are lower than the original power. In the case of decay and increase combination, the instantaneous power after embedding may be higher or lower than the original instantaneous power. Note that the ISM band has a power restriction [13] and thus the average power of the signal has an upper bound. Considering the case of power increase, the average power is absolutely exceeding the upper bound and thus fails to meet the regulation requirement, so we skip the discussion on this case. In this section, we set the parameters of the covert channel $SF_c = 5$, $BW_c = 80Hz$ for illustration.

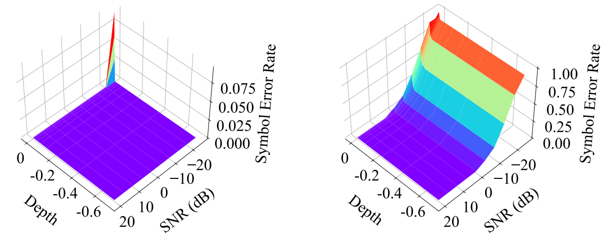
**Power decay.** Fig. 9(a) illustrates the normalized powers of signals with and without decay. We define the difference between the minimum power with embedding and the original power without embedding as *modulation depth*, denoted by $d$. For example, $d = -0.6$ in Fig. 9(a). Fig. 9(b) shows the relationship between modulation depth and the total power ratio of the signal after embedding to the signal before embedding. With the increase in depth, the power ratio increases from 0.56 to 1. When $d = 0$, the power of the signal does not change and thus the power ratio is 1. When $d = -1$, the minimum power is 0 and the average power ratio between it with and without embedding is 0.56, which means the covert chirp uses 56% power of the original chirp.



(a) Decay and increase

(b) Down-depth verse up-depth in decay and increase combination

**Figure 10: Modulation down-depth & up-depth and the relationship between them in the case of decay and increase combination ($SF_c = 5, BW_c = 80Hz$).**



(a) SER with different SNRs with BW=80 Hz

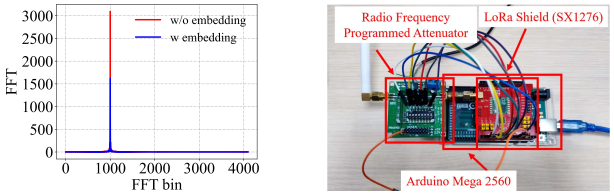
(b) SER with different SNRs with BW=64 kHz

**Figure 11: SER with different SNRs and BWs in the case of decay.**

**Decay and increase combination.** Fig. 10(a) illustrates the relationship between the power with and without the combination of decay and increase after normalization. In this case, the maximum value and minimum value of the signal with embedding are not fixed. We define *down depth* (*down-d*) as the difference value between the original power without embedding and the minimum value with embedding and *up depth* (*up-d*) as the difference value between the maximum value with embedding and the original power without embedding. We adjust *down-d* and *up-d* to ensure the average power with embedding (blue line in Fig. 10(a)) is equal to the original average power of the signal without embedding (red line in Fig. 10(a)). Fig. 10(b) shows the relationship between *down-d* and *up-d* when the average power is equal to the original average power. Just as we can see, with the increase of *down-d*, the minimum value becomes lower and the *up-d* increases. When *down-d* is 1 and the minimum value is lowered to be nearly 0, *up-d* is calculated to be 0.78.

Fig. 11(a) and Fig. 11(b) show the Symbol Error Rate (SER) of the covert channel with different SNRs and $d$s when $SF_c = 5, BW_c = 80$ Hz and $SF_c = 5, BW_c = 64$ kHz, respectively. We can see that with the increase of $d$, SER increases slightly. Therefore, we can conclude that $d$ has a negligible impact on SER.

**Impact on the decoding accuracy.** The power adjusting of the covert channel also affects the decoding accuracy of the legitimate channel. We use an example to help understand its impact. In this example, we set $d = -1$ to let the chirp in the legitimate channel lose as much power as possible. Fig. 12(a) shows the FFT results of the



(a) FFT results of a de-chirped chirp.

(b) Transmitter hardware implementation.

**Figure 12: FFT results and hardware implementation.**

de-chirped chirp of the legitimate channel with and without covert channel embedding. From the figure, we can see that the peak which represents energy accumulation over time after embedding still stands out. It proves to be unaffected on the final symbol distinction because the FFT bin corresponding to the peak is not changed.

## 5.3 Implementation

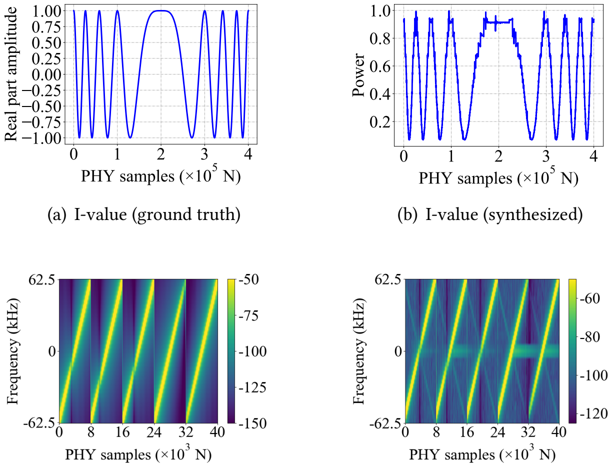
*5.3.1 Hardware.* Although a LoPhy transmitter can be fully implemented using software-defined radio (SDR) devices, e.g., USRP, it is not compatible with existing LoRa end devices. Thus, we implement the LoPhy transmitter using COTS devices to show its feasibility and compatibility.

**Transmitter.** Fig. 12(b) presents the prototype of the LoPhy transmitter. The transmitter consists of three parts, an Arduino Mega microcontroller board [4], a PE43702 7-bit RF Digital Step Attenuator (DSA) [44], and an SX1276-based RFM95 LoRa module [27]. The transmitter uses an omnidirectional antenna with 2 dBi gain. Note that LoPhy only introduces the attenuator as the extra device and does not need any specific hardware modifications. The attenuator covers a band ranging from 9 kHz to 4 GHz, which contains ISM bands utilized by LoRa in different countries and regions. At run time, we use the Arduino to control the attenuator and the LoRa chip simultaneously. The transmitter can be powered by a battery or a power bank.

**Receiver.** The receiver is based on an RTL-SDR v3 [42], a low-cost SDR device, and an omnidirectional antenna with 2 dBi gain. Adopting SDR devices for prototyping is a common practice in the research community [19, 28, 38]. The sampling rate of the RTL-SDR is 1 Msps. We use a Thinkpad-T440p laptop (i7-4700MQ, 2.4GHz, 7.5G RAM) to collect data from the RTL-SDR.

**Cost.** LoPhy requires to equip additional devices on both LoRa gateway and end devices. For the transmitter, LoPhy integrates the attenuator into a standard LoRa end device, which costs about US$20. For the receiver, the price of an RTL-SDR v3 is about US$25.

*5.3.2 Approximate Chirp Synthesization.* The attenuator used in the LoPhy transmitter is a step attenuator covering a 31.75 dB attenuation range in 0.25 dB steps. However, the frequency of a chirp increases or decreases linearly over time, which cannot be achieved by the DSA due to its discrete operation mode. LoPhy addresses this issue by approximate chirp synthesization, i.e., approximating a covert chirp as a sequence of discrete frequency levels, as shown in Fig. 13. The microcontroller adjusts the attenuation depth to create a different amplitude for a certain dwell time, denoted by $\Delta T$. Each legitimate chirp is evenly divided into $\frac{T_{sc}}{\Delta T}$ parts to perform approximate chirp synthesization. In this way, the in-phase value (I value) of the covert chirp is embedded into the amplitude of the legitimate chirp. The shorter the dwell time, the I value of the approximate chirp is more like that of an ideal chirp. After imaginary part generation and de-chirping, the covert chirp can achieve SNR gain as the legitimate chirp. The DSA takes some time when switching to a new attenuation state, which is known as switching speed and settling time. From the datasheet, the total time for switching is about 10.65 $\mu s$. From our empirical measurements, we set the dwell time as 500$\mu s$. Compared with the dwell time used in our setting, the switching time is negligible.



(a) I-value (ground truth)

(b) I-value (synthesized)

(c) Spectrogram (ground truth)

(d) Spectrogram (synthesized)

**Figure 13: Comparison of the ground truth covert chirp and synthesized covert chirp on real devices.**

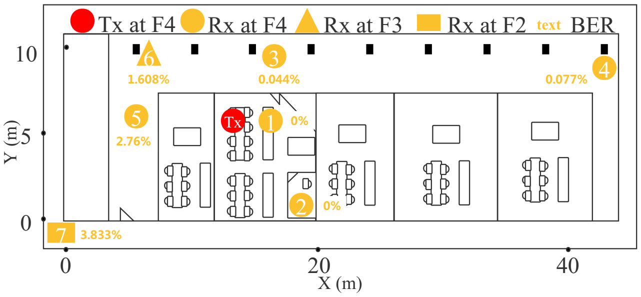


**Figure 14: Indoor experiments deployment and results.**

# 6 EVALUATION

In this section, we conduct extensive experiments and simulations in various settings to evaluate the performance of LoPhy.

## 6.1 Indoor Experiments

**Setup.** We evaluate the performance of LoPhy in a concrete building with four floors. Fig. 14 illustrates the floor plan of the 4th floor. We use our LoPhy prototype as the transmitter to transmit both legitimate and covert messages. We use an RTL-SDR dongle as the

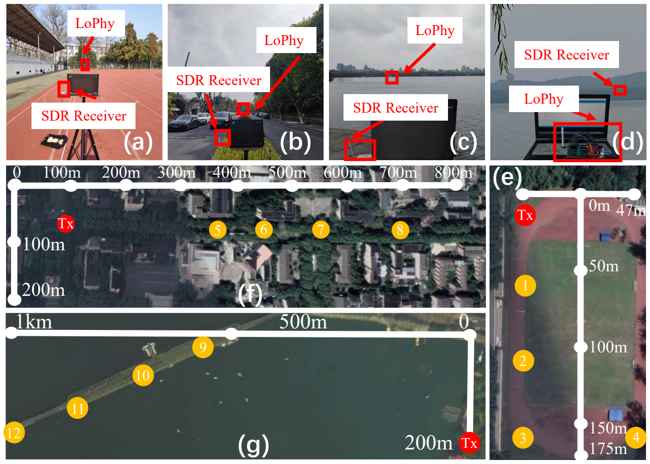


**Figure 15: Outdoor experiments setups: (a) Playground (b) Road (c) Lake-Rx (d) Lake-Tx (e) Playground deployment (f) Road deployment (g) Lake deployment (Image credit: Google Map).**

covert receiver. For the legitimate receiver, we use a COTS LoRa end device. We set $SF = 12, BW = 125kHz$ for the legitimate channel and $SF_c = 5, BW_c = 80Hz$ for the covert channel. The transmission power of LoPhy transmitter is 20 dBm and the receive gain of the covert receiver is 49.6 dB. We adopt a power decay of $d = -1$ for the power adjustment. The dwell time $\Delta T$ of the DSA is set to be $500\mu s$. We set the default sampling rate of the covert channel receiver as 1 MHz. The *payload* of the covert message consists of 48-bit useful information. In addition to the *sync word* before *payload* which is 10-bit, the total length of the LoPhy frame is 58 bits.

We deploy the transmitter in a lab on the 4th floor. Then, we carry the receiver to seven different locations, as shown in Fig. 14. The locations represented by yellow circles (#1-#5) are on the same floor as the transmitter. The locations represented by the yellow triangle (#6) and the yellow rectangle (#7) are on the 3rd floor and 2nd floor, respectively. At each location, the transmitter sends 100 packets. We use Bit Error Rate (BER) to measure the covert channel communication performance and Symbol Error Rate (SER) to measure the impact on the legitimate channel.

**Results.** Fig. 14 presents the BER of the covert communication at different locations. The BER is 0% when the receiver is at location #1 and #2 because the transceivers are in the same lab and have line-of-sight (LOS) propagation paths. The BER increases when there are more obstacles between the transmitter and the receiver due to extensive non-line-of-sight (NLOS) propagation. Additionally, the SER of the legitimate LoRa remains 0% at each location, which means that LoPhy does not affect the legitimate channel transmission in this experiment.

## 6.2 Outdoor Experiments

**Setup.** We conduct the experiments in different outdoor environments to evaluate the performance of LoPhy at different distances. We conduct experiments at a playground (Fig. 15(a)), along a road (Fig. 15(b)), and by a lake (Fig. 15(c, d)). The parameters of the legitimate channel and covert channel are all same as that of indoor experiments. The transmitter and the receivers are placed on tripods during the experiments.

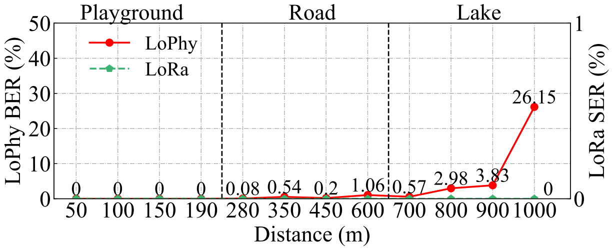


**Figure 16: Outdoor experiments results.**

For the experiments at the playground, as shown in Fig. 15(d), we fix the position of the transmitter and carry the receivers to different locations, which are 50 m, 100 m, 150 m, and 190 m away from the transmitter, respectively. For the experiments along the road, as shown in Fig. 15(e), we fix the position of the transmitter and move the receivers to visit four positions, which are 280 m, 350 m, 450 m, and 600 m away from the transmitter, respectively. There are a lot of moving and still obstacles on and along the road, including vehicles, passengers, and trees. For the experiments by the lake, as shown in Fig. 15(f), we fix the position of the transmitter and move the receivers to four positions, which are 700 m, 800 m, 900 m, and 1000 m away from the transmitter, respectively. The electromagnetic waves travel on the lake with no obstacles other than a few boats. At each location, the transmitter sends 100 packets. We then measure the BER of LoPhy and the SER of LoRa at each location.

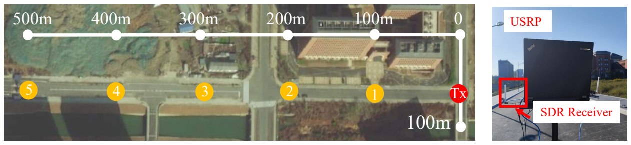
**Results.** Fig. 16 presents the BER of the covert communication and SER of the legitimate communication of different distances. As we can see, the BER of LoPhy is 0% on the playground. On the road, the BER is very low and shows a winding upward trend with the distance. When by the lake, LoPhy presents a BER of less than 4% at 700 m, 800 m, and 900 m. The BER increases to 26.15% at 1, 000 m. To investigate this issue, we check the Received Signal Strength Indication (RSSI) of the signal. The RSSI at 700 m, 800 m, 900 m, and 1 km are −100 dB, −108 dB, −113 dB, and −126 dB, respectively. As we can see, the received signal strength decreases with long propagation distances, which indicates that the signal suffers more attenuation and interference.

The SER of the legitimate LoRa remains 0% at each location, which means that LoPhy does not affect the legitimate channel transmission in the experiments.

## 6.3 Comparison with State-of-the-art System

We compare LoPhy with CloakLoRa [29], which is the state-of-the-art system, through field experiments and simulations to understand: (1) their impacts on the performance of the legitimate channel; and (2) their BERs and throughputs; and (3) their SERs in different SNRs. Since CloakLoRa is not publicly available, we reproduce it according to [29].

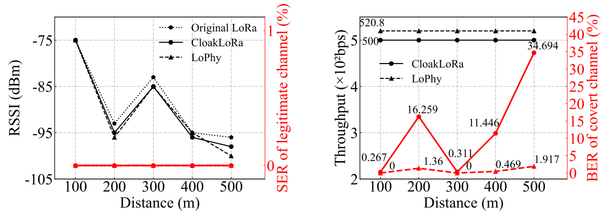
*6.3.1 Experiments.* To fairly compare these two approaches, we adopt the same setting for the legitimate channel, i.e., $SF = 8$,



(a) The deployment of comparative experiments on the road (Image credit: Google Map)

(b) Road

**Figure 17: Comparative experiments setups.**



(a) Impact on legitimate channel

(b) Performance of covert channel

**Figure 18: Performance comparison between LoPhy and CloakLoRa.**

$BW = 250$ kHz. Also, we need to make the throughput of these two methods as close as possible. Thus, we set $SF_c = 5$, $BW_c = 80$ Hz, and $d = -0.9$ for LoPhy. For CloakLoRa, we adopt its default setting. As a result, throughputs of LoPhy and CloakLoRa are 520.8 bps and 500 bps, respectively.

As shown in Fig. 17(a), we conduct experiments at distances of 100 m, 200 m, 300 m, 400 m, and 500 m. We use USRP B210 [46] as Tx and RTL-SDR dongle as Rx. The Tx power is set to 17 dBm, and Rx gain is set to 30 dB. At each location, we send 100 packets using LoRa (without covert embedding), LoPhy, and CloakLoRa, respectively. The payload length of LoPhy and CloakLoRa is 50 bits. We then measure Packet Delivery Ratio (PDR), RSSI, SER of the legitimate channel, and BER of the covert channel.

**Results.** Fig. 18(a) illustrates the impact of LoPhy and CloakLoRa on legitimate channel. Compared with the original LoRa, we can see that both LoPhy and CloakLoRa weaken the RSSI of the legitimate channel but do not affect the decoding accuracy of the legitimate channel across all distances. For PDR, they are all 100%. Fig. 18(b) shows that LoPhy has a lower BER at every distance compared with CloakLoRa, which means that LoPhy is more resilient to noise. Note that CloakLoRa has a 36.694% BER when the transmission distance is 500 m while LoPhy only has a 1.917% BER.

*6.3.2 Simulations.* We conduct some simulations using GNU Radio [32], a software that provides signal processing blocks to implement software-defined radios and signal-processing systems, to measure the SER of the covert channel under different SNR settings. We add Additive White Gaussian Noise (AWGN) to the signal to quantitatively measure the impact of noise on the SER. Fig. 19(a) presents the SER of the covert channel with different SNRs. Different lines represent different bit rate settings of the covert channel. As we can see, LoPhy maintains 0% SER when SNR is higher than −5 dB. If we lower the bit rate, e.g., *bit rate* = 200 bps, the proposed covert channel can be super resilient. In contrast, CloakLoRa cannot maintain a low SER when SNR is lower than 0 dB even the bit rate is lowered to 200 bps. We compare the noise resistance of LoPhy and CloakLoRa at the same bit rate by calculating the SNR under which they reach 0% SER. As is shown in Fig. 19(a), they respectively achieve 0% SER at SNR of −15 dB and 3 dB at the same bit rate of 200 bps. In conclusion, LoPhy has about 63× ($10^{\frac{3}{10}}/10^{\frac{-15}{10}} = 63.0957$) gain on noise resilience.

## 6.4 Numerical Study

Due to hardware limitations such as the dwell time of DSA, the LoPhy prototype does not support all parameters. To understand the performance limits of LoPhy, we further implement LoPhy in GNU Radio. Specifically, we conduct experiments to explore the maximum covert channel bandwidth, and the maximum covert channel bit rate.

**Maximum bandwidth of the covert channel.** In CSS modulation, the bandwidth affects the maximum bit rate when the sampling rate of the SDR receiver is fixed. Thus, it is important to learn the maximum covert channel bandwidth. The sample numbers per symbol, denoted by $N_s$, can be expressed by

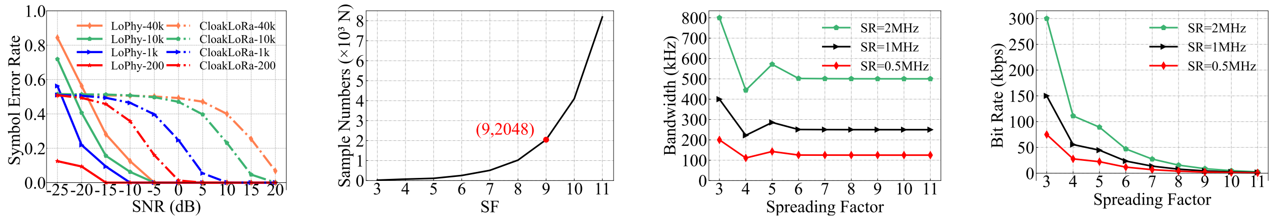
$$N_s = sr_s \cdot T_{sc} = sr_s \cdot \frac{2^{SF_c}}{BW_c}, \tag{15}$$

where $sr_s$ denotes the sampling rate of the SDR receiver and $T_{sc}$ represents the symbol time in the covert channel. For an SDR receiver, its sampling rate $sr_s$ is fixed when receiving the signal, which can be taken as a constant. Thus, in Eq. 15, given a fixed $sr_s$ and $SF_c$, the sample numbers per symbol $N_s$ is the decisive factor and inversely proportional to $BW_c$. Note that $N_s$ has a lower bound to ensure the decoding accuracy of the covert channel. Mathematically, CSS requires at least $2^{SF_c}$ sample points per chirp to perform an FFT to recover the initial frequency. Then, we compute the sample numbers per symbol point by point for each spreading factor to get the minimum value that can meet the requirement of BER equal to 0 by simulation. Fig. 19(b) presents the simulation results when the receiver has a sampling rate $sr_s$ of 1 MHz. For example, if the receiver receives a covert chirp with no less than 2,048 sample points when $SF_c = 9$, it can decode the chirp correctly. What's more, we can find that the relationship between $2^{SF_c}$ and the minimum sample per symbol in Fig. 19(b) verifies the Nyquist's theorem [57]. Therefore, according to Eq. 15 and Nyquist's theorem, if we want to achieve a larger bandwidth for a certain spreading factor $SF_c$, we can increase the sampling rate $sr_s$ of the receiver. Fig. 19(c) shows the maximum bandwidth of different spreading factors when the receiver has different sampling rates. If we use a receiver with 1 MHz sampling rate, the maximum bandwidth of the covert channel is about 250 kHz across all spreading factors.

**Maximum bit rate of the covert channel.** The bit rate of the covert channel can be expressed by

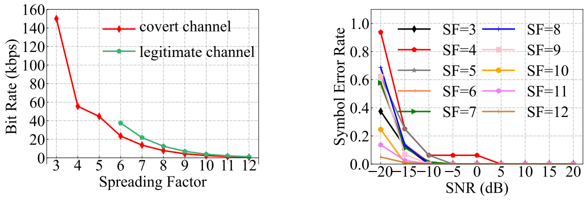
$$bit\ rate = \frac{SF_c}{T_{sc}} = \frac{SF_c}{(\frac{2^{SF_c}}{BW_c})} = BW_c \cdot \frac{SF_c}{2^{SF_c}}, \tag{16}$$

where $SF_c$ is the spreading factor, $T_{sc}$ is the symbol time, and $BW_c$ is the bandwidth. The *bit rate* is numerically proportional to the bandwidth $BW_c$ and related to spreading factor $SF_c$. Based on the previous results of maximum bandwidth, we can calculate the maximum bit rate of different spreading factors accordingly, as shown in Fig. 19(d). The covert channel can reach a maximum bit rate of 150 kbps with $sr_s = 1$ MHz and $SF_c = 3$. The maximum bit rate



(a) SER comparison (b) Minimum sample-per-symbol (c) Maximum bandwidth (d) Maximum bit rate

**Figure 19: SER comparison of LoPhy and CloakLoRa and simulation results of the minimum sample per symbol, maximum bandwidth, and maximum bit rate of the LoPhy.**



(a) Bit rate of different channels. (b) SER of the covert channel.

**Figure 20: Bit rate of different channels and SER of the covert channel.**

decreases with the increase of $SF_c$. Same as the bandwidth, the bit rate is proportional to the sampling rate $sr_s$ of the receiver. Thus, the maximum bit rate changes for a certain spreading factor with the sampling rate accordingly.

## 7 LOPHY ENABLED APPLICATIONS

While an adversary might attempt to exploit LoPhy by gaining physical access to the LoRa devices in order to leak information, this is not our primary use case for the covert channel. Instead, we envision the channel being utilized by cooperative applications to send additional information. In this section, we demonstrate the potential applications that can be enabled by LoPhy, including channel aggregation and data timestamping.

**Channel aggregation.** LoPhy boosts the data rate of LoRa by aggregating the legitimate channel and covert channel. If both channels are known by the transceiver, the user can utilize them for data transmission. The maximum data rate of LoRa's legitimate channel ranges from 1, 171 bps to 37, 500 bps in various sets of parameters [48]. Fig. 20(a) illustrates the maximum data rates of the legitimate channel and the covert channel using different settings. We can see that, if the user can aggregate the two channels, the data rate can be boosted significantly. Note that the parameter setting (e.g., SF) of the legitimate channel does not affect the covert channel because the covert channel modulates on the power amplitude of the legitimate channel signal. Thus, the user can configure the covert channel according to SNR conditions to boost the data rate.

We also demonstrate some simulations in GNU Radio to explore the SER of the covert channel with different SFs and data rates at different SNRs. The simulation parameters are set to be SFs and their corresponding maximum bit rate. Fig. 20(b) shows the results and it illustrates that the SER of the covert channel in different SFs can be very low and it is nearly 0% when SNR is not less than -10dB which is enough to communicate for long distances in real circumstances. According to the analysis, we build a reliable and super resilient covert channel over LoRa's PHY and it can improve LoRa's original communication rate largely. It can be used in the smart industry to transmit more sensor data at a low cost.

**Data Timestamping.** Data timestamping helps record the time of interest in terms of wall clock, which is a basic system function required by data collection applications for monitoring. In LoRa, there are two approaches to achieving data timestamping, i.e., sync-based and sync-free [21]. Specifically, for the sync-based approach, the end nodes are synchronized to the global time using clock synchronization protocols. Time synchronization helps correct the clock drift of the end device so that the end device can timestamp the sensor measurement locally. However, clock synchronization introduces considerable communication overhead to LoRaWAN due to its limited bandwidth. The sync-free approach avoids the communication overhead by sending the data once generated. However, the sync-free approach is not applicable to all applications and is vulnerable to replay attacks [49].

LoPhy balances the efficiency and security of data timestamping in LoRaWAN by encoding the data timestamp in the covert channel. LoPhy end node transmits the message and the timestamp using the legitimate channel and covert channel, respectively. The gateway decodes the payload and the timestamp accordingly.

## 8 RELATED WORK

**Covert channels.** The covert channel exploits the physical properties of the legitimate channel to transmit data that can bypass network security inspection [33]. Prior studies leverage a broad spectrum of mediums to design covert channels, including multimedia content [31], wired network protocols [1, 6, 34], wireless communication [11, 14, 20], thermal emanation [25], acoustic emanation [26], electromagnetic radiation [50], and backscatter [60]. Specifically, some recent works implement wireless covert channels by hacking the passband modulation techniques, e.g., OFDM [54], constellation-based modulation [7, 12]. For example, introducing an artificial CFO in OFDM can create a physical layer covert channel in Wi-Fi [11]. However, these works are not applicable for LoRa, which has a longer transmission distance and unique modulation scheme.

The most related work to LoPhy is CloakLoRa [29], which modulates the amplitudes of LoRa chirps which is orthogonal to CSS, to embed covert information into a legitimate LoRa packet while the frequency of the signal is not changed. However, CloakLoRa adopts the OOK modulation scheme, which is known as not resilient to noise and has a limited communication range. Differently, LoPhy utilizes CSS modulation to boost the communication range of the covert channel.

**LoRa/LoRaWAN.** As a promising and state-of-the-art physical layer wireless standard for LPWAN, LoRa has attracted increasing attention both from academia and industry. Researchers have devoted significant efforts to improving the communication performance or enabling new applications of LoRa and its data link layer specification, i.e., LoRaWAN. To improve communication performance, existing studies adopt various techniques to modify the physical layer or design new MACs, e.g., collisions resolving [10, 36, 58], low-SNR demodulation [35], carrier-sense multiple access, and parameter optimization [15, 18, 53]. To enable new applications beyond communication, researchers investigate the physical properties or employ advanced signal processing techniques, e.g., end device localization [5, 22, 30, 39], cross-technology communication [37, 40, 51], wireless sensing [59, 62], and backscatter [23, 24, 43].

Different from prior studies of LoRa, LoPhy builds a resilient and high throughput covert channel over LoRa PHY. LoPhy modulates covert chirps into the amplitude of LoRa signals without affecting the legitimate channel. LoPhy further challenges the common belief that the covert channel is a security threat by demonstrating two specific applications, which improve the throughput and energy efficiency of LoRa.

## 9 DISCUSSION

**Coexistence with the security mechanism.** We observe that current LoRaWAN secures the application layer and network layer with symmetric encryption and it does not examine physical layer communication parameters, therefore the amplitude change of PHY does not affect the security mechanism.

**Good or evil?** The network admin may propose a countermeasure if prior knowledge of LoPhy is available. From our experiment results, the existing LoRa end devices cannot detect LoPhy by simply inspecting the performance of the legitimate channel. Although covert channels have been viewed as a type of malicious attack for a long time, there are some research works that leverage covert channels to create an out-of-band channel for system security enhancement [55, 61]. Our work is primarily motivated by scenarios where the "covert" channel is used by cooperative agents to augment the communication of legitimate applications, as opposed to being used by an adversary. As presented in §7, LoPhy enables new applications that improve the performance of the legitimate channel. The theoretical and experimental results call for further research on rethinking the use of the covert channel in LPWAN.

**Error detection and correction.** We append Cyclic Redundancy Check (CRC) to the *payload* to detect the transmission error. The results show that all errors can be detected by CRC within the range of 900 m. Although we can implement an error detection and retransmission scheme for LoPhy with CRC, it is desirable to design an error correction scheme to reduce retransmission. We leave this issue for our future work.

## 10 CONCLUSION

We present LoPhy, a new covert channel over LoRa physical layer, which is super resilient to noise and has high throughput. We implement the proposed covert channel on COTS LoRa end devices and conduct extensive experiments and simulations to evaluate its performance. Compared with the state-of-the-art covert channel implementation over LoRa PHY (i.e., CloakLoRa), LoPhy brings significant performance improvements in terms of noise resilience and bit error reduction. By achieving this, LoPhy further enables new applications for LoRa to improve its throughput and save energy. These results call for further research on leveraging the covert channel to improve the performance of the legitimate channel.

## ACKNOWLEDGMENTS

Thank Prof. Rui Tan, Prof. Mo Li, Prof. Li Chai, and Dr. Kang Hu for their insightful discussions. Thank Yuchen Miao, Kecheng Qin, Huajian Zhou, and Lei Zheng for helping conduct experiments. Thank the anonymous reviewers and Shepherd for the valuable comments. This work is supported in part by the National Science Foundation of China (NSFC) under Grant No. U1909207, and in part by NSFC under Grants 62293510/62293511. Chaojie Gu is the corresponding author.

## REFERENCES

[1] Kamran Ahsan. 2002. Covert channel analysis and data hiding in TCP/IP. (01 2002).

[2] LoRa Alliance. March 7, 2023. A technical overview of LoRa and LoRaWAN. https://lora-alliance.org/resource-hub/what-lorawanr

[3] Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence, and Danny Hughes. 2017. Exploring the Security Vulnerabilities of LoRa. In *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*.

[4] Arduino. March 7, 2023. Arduino Mega 2560 Rev3. http://store.arduino.cc/products/arduino-mega-2560-rev3

[5] Atul Bansal, Akshay Gadre, Vaibhav Singh, Anthony Rowe, Bob Iannucci, and Swarun Kumar. 2021. Owll: Accurate lora localization using the tv whitespaces. In *Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021)*. 148–162.

[6] Serdar Cabuk, Carla E. Brodley, and Clay Shields. 2009. IP Covert Channel Detection. *ACM Trans. Inf. Syst. Secur.* 12, 4, Article 22 (apr 2009), 29 pages. https://doi.org/10.1145/1513601.1513604

[7] Pengcheng Cao, Weiwei Liu, Guangjie Liu, Xiao-Peng Ji, Jiangtao Zhai, and Yuewei Dai. 2018. A Wireless Covert Channel Based on Constellation Shaping Modulation. *Security and Communication Networks* 2018 (01 2018), 1–15. https://doi.org/10.1155/2018/1214681

[8] Marco Centenaro, Lorenzo Vangelista, Andrea Zanella, and Michele Zorzi. 2016. Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications* 23, 5 (2016), 60–67. https://doi.org/10.1109/MWC.2016.7721743

[9] Smilty Chacko and Mr. Deepu Job. 2018. Security mechanisms and Vulnerabilities in LPWAN. *IOP Conference Series: Materials Science and Engineering* 396 (aug 2018), 012027. https://doi.org/10.1088/1757-899x/396/1/012027

[10] Qian Chen and Jiliang Wang. 2021. AlignTrack: Push the Limit of LoRa Collision Decoding. In *2021 IEEE 29th International Conference on Network Protocols (ICNP)*. IEEE, 1–11.

[11] Jiska Classen, Matthias Schulz, and Matthias Hollick. 2015. Practical covert channels for WiFi systems. In *2015 IEEE Conference on Communications and Network Security (CNS)*. 209–217. https://doi.org/10.1109/CNS.2015.7346830

[12] Aveek Dutta, Dola Saha, Dirk Grunwald, and Douglas Sicker. 2012. Secret agent radio: Covert communication through dirty constellations. In *International Workshop on Information Hiding*. Springer, 160–175.

[13] FCC. March 7, 2023. PART 18 - INDUSTRIAL, SCIENTIFIC, AND MEDICAL EQUIPMENT. https://www.ecfr.gov/current/title-47/part-18

[14] Lilia Frikha, Zouheir Trabelsi, and Wassim El-Hajj. 2008. Implementation of a Covert Channel in the 802.11 Header. In *2008 International Wireless Communications and Mobile Computing Conference*. 594–599.

[15] Akshay Gadre, Revathy Narayanan, Anh Luong, Anthony Rowe, Bob Iannucci, and Swarun Kumar. 2020. Frequency Configuration for Low-Power Wide-Area

Networks in a Heartbeat. In *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*. 339–352.

[16] Akshay Gadre, Fan Yi, Anthony Rowe, Bob Iannucci, and Swarun Kumar. 2020. Quick (and Dirty) Aggregate Queries on Low-Power WANs. In *2020 19th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. 277–288. https://doi.org/10.1109/IPSN48710.2020.00031

[17] Amalinda Gamage, Jansen Christian Liando, Chaojie Gu, Rui Tan, and Mo Li. 2020. *LMAC: Efficient Carrier-Sense Multiple Access for LoRa*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3372224.3419200

[18] Weifeng Gao, Wan Du, Zhiwei Zhao, Geyong Min, and Mukesh Singhal. 2019. Towards energy-fairness in lora networks. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 788–798.

[19] Cristinel Gavrilă, Csaba-Zoltan Kertesz, Marian Alexandru, and Vlad Popescu. 2018. Reconfigurable IoT gateway based on a SDR platform. In *2018 International Conference on Communications (COMM)*. IEEE, 345–348.

[20] Krystian Grzesiak, Zbigniew Piotrowski, and Jan M. Kelner. 2021. A Wireless Covert Channel Based on Dirty Constellation with Phase Drift. *Electronics* 10, 6 (2021). https://www.mdpi.com/2079-9292/10/6/647

[21] Chaojie Gu, Linshan Jiang, Rui Tan, Mo Li, and Jun Huang. 2021. Attack-aware synchronization-free data timestamping in lorawan. *ACM Transactions on Sensor Networks (TOSN)* 18, 1 (2021), 1–31.

[22] Dongfang Guo, Chaojie Gu, Linshan Jiang, Wenjie Luo, and Rui Tan. 2022. ILLOC: In-Hall Localization with Standard LoRaWAN Uplink Frames. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* (2022).

[23] Xiuzhen Guo, Longfei Shangguan, Yuan He, Nan Jing, Jiacheng Zhang, Haotian Jiang, and Yunhao Liu. 2022. Saiyan: Design and Implementation of a Low-power Demodulator for {LoRa} Backscatter Systems. In *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*. 437–451.

[24] Xiuzhen Guo, Longfei Shangguan, Yuan He, Jia Zhang, Haotian Jiang, Awais Ahmad Siddiqi, and Yunhao Liu. 2020. *Aloba: Rethinking ON-OFF Keying Modulation for Ambient LoRa Backscatter*. Association for Computing Machinery, 192–204.

[25] Mordechai Guri, Matan Monitz, Yisroel Mirski, and Yuval Elovici. 2015. BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations. In *2015 IEEE 28th Computer Security Foundations Symposium*.

[26] Michael Hanspach and Michael Goetz. 2014. On Covert Acoustical Mesh Networks in Air. *Journal of Communications* 8 (06 2014). https://doi.org/10.12720/jcm.8.11.758-767

[27] Ltd. HOPE Microelectronics CO. March 7, 2023. RFM95W LoRa Module. https://www.hoperf.com/modules/lora/RFM95.html

[28] Ningning Hou, Xianjin Xia, and Yuanqing Zheng. 2021. Jamming of LoRa PHY and countermeasure. In *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*. IEEE, 1–10.

[29] Ningning Hou and Yuanqing Zheng. 2020. Cloaklora: A covert channel over LoRa phy. In *2020 IEEE 28th International Conference on Network Protocols (ICNP)*. IEEE, 1–11.

[30] Kang Hu, Chaojie Gu, and Jiming Chen. 2022. LTrack: A LoRa-Based Indoor Tracking System for Mobile Robots. *IEEE Transactions on Vehicular Technology* 71, 4 (2022), 4264–4276. https://doi.org/10.1109/TVT.2022.3143526

[31] Hassan Khan, Mobin Javed, Syed Ali Khayam, and Fauzan Mirza. 2011. Designing a cluster-based covert channel to evade disk investigation and forensics. *Computers & Security* 30, 1 (2011), 35–49. https://doi.org/10.1016/j.cose.2010.10.005

[32] Matthew Knight and Balint Seeber. 2016. Decoding LoRa: Realizing a Modern LPWAN with SDR.

[33] Butler W Lampson. 1973. A note on the confinement problem. *Commun. ACM* 16, 10 (1973), 613–615.

[34] Ki Suh Lee, Han Wang, and Hakim Weatherspoon. 2014. PHY Covert Channels: Can you see the Idles?. In *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*. USENIX Association, Seattle, WA, 173–185.

[35] Chenning Li, Hanqing Guo, Shuai Tong, Xiao Zeng, Zhichao Cao, Mi Zhang, Qiben Yan, Li Xiao, Jiliang Wang, and Yunhao Liu. 2021. NELoRa: Towards Ultra-low SNR LoRa Communication with Neural-enhanced Demodulation. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*. 56–68.

[36] Chenning Li, Xiuzhen Guo, Longfei Shangguan, Zhichao Cao, and Kyle Jamieson. 2022. CurvingLoRa to Boost LoRa Network Throughput via Concurrent Transmission. In *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*.

[37] Zhijun Li and Yongrui Chen. 2020. BLE2LoRa: cross-technology communication from bluetooth to LoRa via chirp emulation. In *2020 17th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 1–9.

[38] Jansen C Liando, Amalinda Gamage, Agustinus W Tengourtius, and Mo Li. 2019. Known and unknown facts of LoRa: Experiences from a large-scale measurement study. *ACM Transactions on Sensor Networks (TOSN)* 15, 2 (2019), 1–35.

[39] Jun Liu, Jiayao Gao, Sanjay Jha, and Wen Hu. 2021. Seirios: leveraging multiple channels for LoRaWAN indoor and outdoor localization. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. 656–669.

[40] Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, and Tian He. 2020. Xfi: Cross-technology iot data collection via commodity wifi. In *2020 IEEE 28th International Conference on Network Protocols (ICNP)*. IEEE, 1–11.

[41] Jorge Navarro-Ortiz, Natalia Chinchilla-Romero, Juan J. Ramos-Munoz, and Pablo Munoz-Luengo. 2019. Improving Hardware Security for LoRaWAN. In *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*. 1–6. https://doi.org/10.1109/CSCN.2019.8931397

[42] Osmocom. March 7, 2023. RTL-SDR v3. https://osmocom.org/projects/rtl-sdr/wiki/Rtl-sdr

[43] Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle Jamieson. 2018. PLoRa: A passive long-range data network from ambient LoRa transmissions. In *Proceedings of the 2018 conference of the ACM special interest group on data communication*. 147–160.

[44] pSemi Corp. March 7, 2023. PE43702. https://www.digchip.com/datasheets/parts/datasheet/358/PE43702-pdf.php

[45] ABI Research. March 7, 2023. NB-IoT and LTE-M Issues to Boost LoRa and Sigfox Near and Long-term Lead in LPWA Network Connections. https://tinyurl.com/2026-cellular-iot

[46] Ettus Research. 2022. USRP B210 Datasheet. https://www.ettus.com/wp-content/uploads/2019/01/b200-b210_spec_sheet.pdf

[47] Pieter Robyns, Peter Quax, Wim Lamotte, and William Thenaers. 2018. A Multi-Channel Software Decoder for the LoRa Modulation Scheme.. In *IoTBDS*. 41–51.

[48] Semtech. 2020. SX1276/77/78/79 Datasheet. https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/2R0000001Rbr/6EfVZUorrpoKFfvaF_Fkpgp5kzjiNyiAbqcpqh9qSjE

[49] Jothi Prasanna Shanmuga Sundaram, Wan Du, and Zhiwei Zhao. 2020. A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues. *IEEE Communications Surveys Tutorials* 22, 1 (2020), 371–388.

[50] Cheng Shen, Tian Liu, Jun Huang, and Rui Tan. 2021. When LoRa meets EMR: Electromagnetic covert channels can be super resilient. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1304–1317.

[51] Junyang Shi, Di Mu, and Mo Sha. 2019. Lorabee: Cross-technology communication from lora to zigbee via payload encoding. In *2019 IEEE 27th International Conference on Network Protocols (ICNP)*. IEEE, 1–11.

[52] Weightless SIG. March 7, 2023. Weightless Specification. http://www.weightless.org/about/weightless-specification

[53] Yuyi Sun, Jiming Chen, Shibo He, and Zhiguo Shi. 2021. High-Confidence Gateway Planning and Performance Evaluation of a Hybrid LoRa Network. *IEEE Internet of Things Journal* 8, 2 (2021), 1071–1081. https://doi.org/10.1109/JIOT.2020.3011139

[54] Krzysztof Szczypiorski and Wojciech Mazurczyk. 2010. Hiding data in OFDM symbols of IEEE 802.11 networks. In *2010 International Conference on Multimedia Information Networking and Security*. IEEE, 835–840.

[55] James M. Taylor and Hamid R. Sharif. 2017. Enhancing integrity of modbus TCP through covert channels. In *2017 11th International Conference on Signal Processing and Communication Systems (ICSPCS)*. 1–6.

[56] Shuai Tong, Jiliang Wang, and Yunhao Liu. 2020. Combating Packet Collisions Using Non-Stationary Signal Scaling in LPWANs. In *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services* (Toronto, Ontario, Canada) *(MobiSys '20)*. Association for Computing Machinery, New York, NY, USA, 234–246. https://doi.org/10.1145/3386901.3388913

[57] Martin H. Weik. 2001. *Nyquist theorem*. Springer US, Boston, MA, 1127–1127. https://doi.org/10.1007/1-4020-0613-6_12654

[58] Xianjin Xia, Ningning Hou, Yuanqing Zheng, and Tao Gu. 2021. PCube: scaling LoRa concurrent transmissions with reception diversities. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*.

[59] Binbin Xie, Yuqing Yin, and Jie Xiong. 2021. Pushing the Limits of Long Range Wireless Sensing with LoRa. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 3, Article 134 (sep 2021), 21 pages. https://doi.org/10.1145/3478080

[60] Zhice Yang, Qianyi Huang, and Qian Zhang. 2017. Nicscatter: Backscatter as a covert channel in mobile devices. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*. 356–367.

[61] Xuhang Ying, Giuseppe Bernieri, Mauro Conti, and Radha Poovendran. 2019. TACAN: Transmitter Authentication through Covert Channels in Controller Area Networks. In *Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS '19)*. New York, NY, USA, 23–34.

[62] Fusang Zhang, Zhaoxin Chang, Jie Xiong, Rong Zheng, Junqi Ma, Kai Niu, Beihong Jin, and Daqing Zhang. 2021. Unlocking the Beamforming Potential of LoRa for Long-Range Multi-Target Respiration Sensing. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 2, Article 85 (jun 2021), 25 pages. https://doi.org/10.1145/3463526