LoPhy
A Resilient and Fast Covert Channel over LoRa PHY

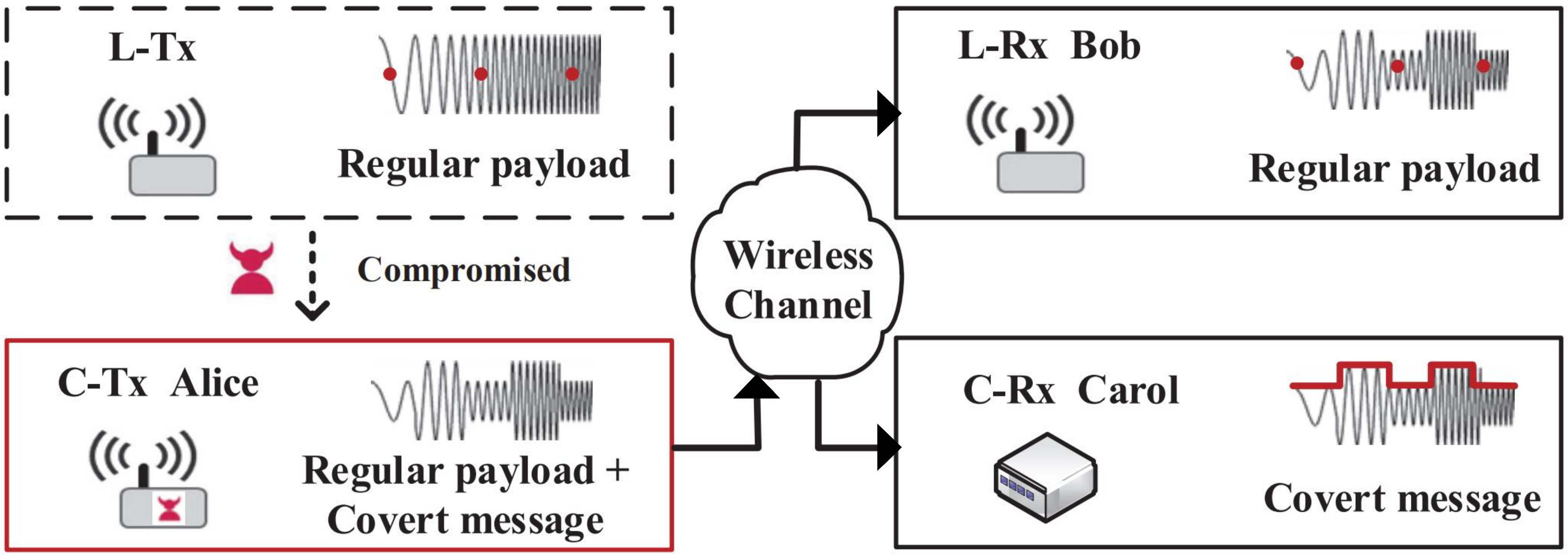
Boya Liu, Chaojie Gu, Shibo He, Jiming Chen

Zhejiang University, China

IPSN’23

ZHEJIANG UNIVERSITY

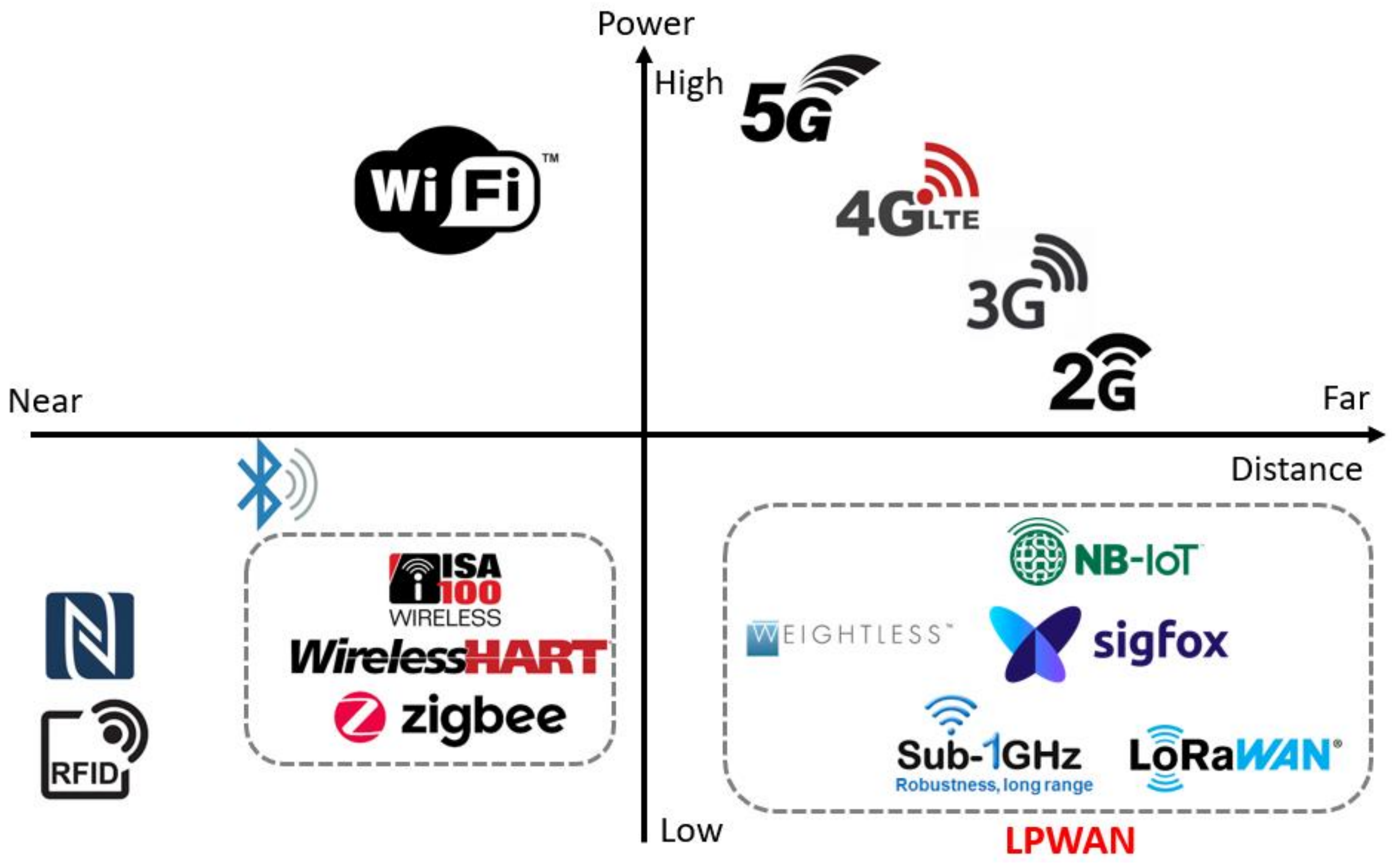
Covert Channel



- The legitimate receiver can decode the legitimate payload (i.e., Bob) but it will not check the covert channel.

- Image credits: Ningning Hou, Yuanqing Zheng, "CloakLoRa: A Covert Channel over LoRa PHY", In IEEE ICNP, Madrid, Spain, Oct 13-16, 2020

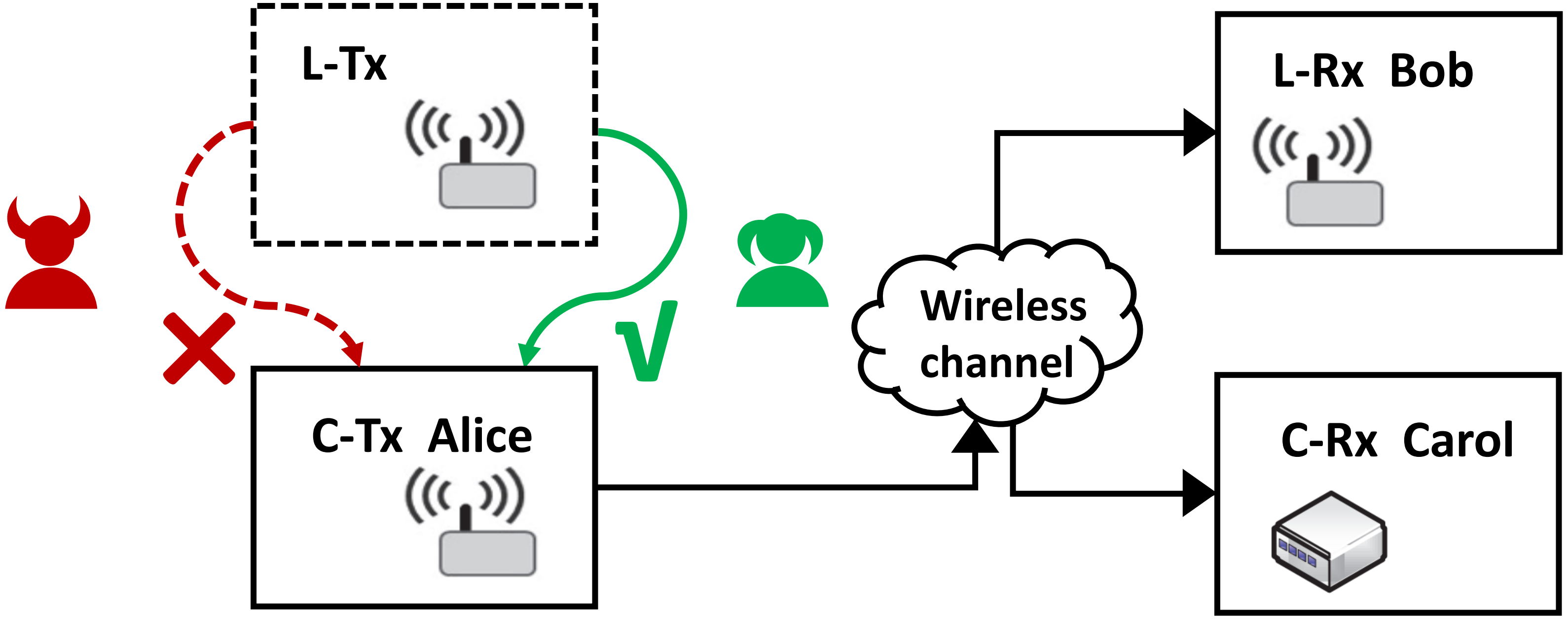
Low Power Wide Area Networks



- LPWAN
  - Long-range communication
  - Low power consumption
- LoRaWAN
  - Open data link standard
  - Use of license free ISM band

- There are **not many studies** about covert channels in LPWAN.
- There are also some researchers working on it.

Covert Channel



Covert channel can be…

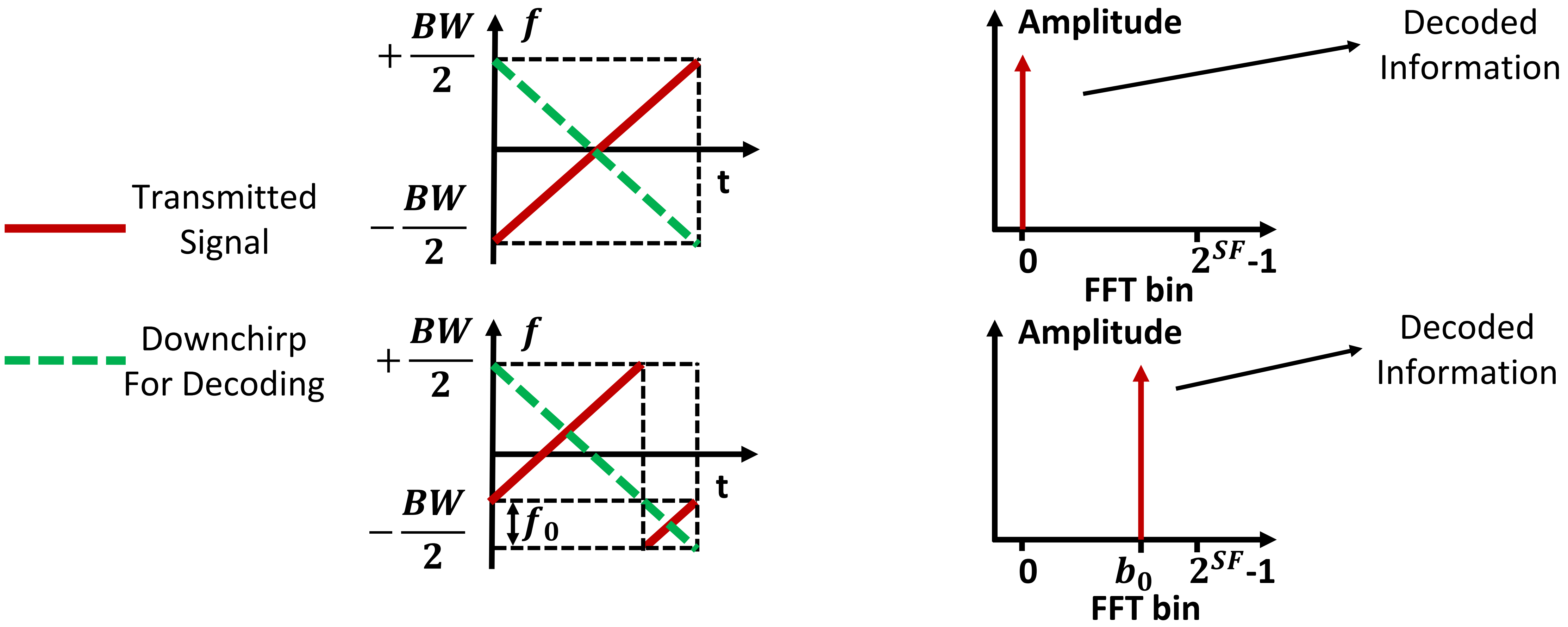
× Adversaries: break protections and leak information

✓ Cooperative agents: improve the performance

Related Work

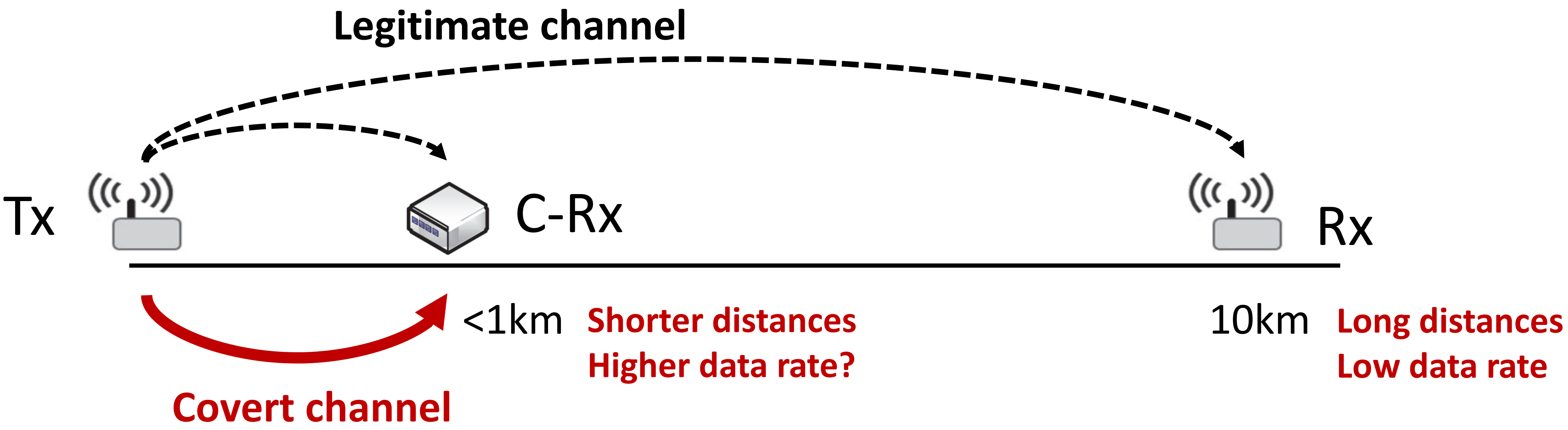
- CloakLoRa [ICNP’20]
  - AM modulation
  - 250 m communication range
  - Low data rate
- EMLoRa [SP’21]
  - Electromagnetic (EM) signals leaked from PC/laptops
  - Chirp Spread Spectrum (CSS) modulation
  - Longer communication range than other EM covert channels
- LoPhy (LPWAN over LoRa PHY) [This work]
  - “ CSS modulation ” on amplitude
  - Resilient
  - Higher date rate
  - Compatible with COTS LoRa end devices

LoRa PHY: Chirp Spread Spectrum (CSS)



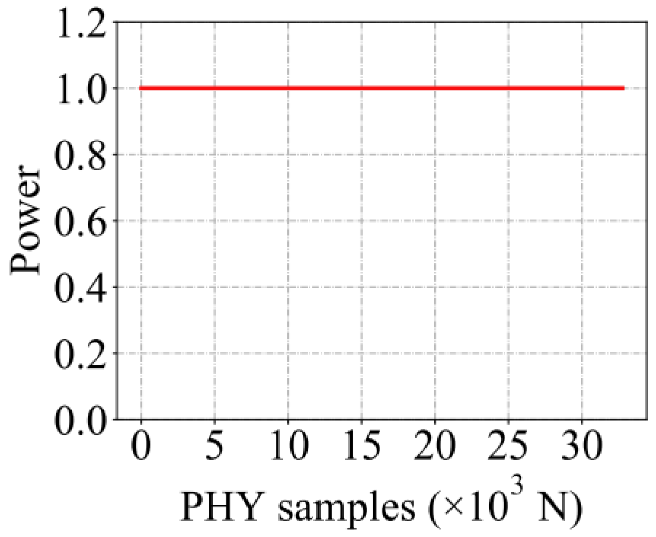
- The receiver can multiply the received signal with a down-chirp to **converge the energy spreading over the entire bandwidth** to get SNR gain.

Trade-off between Capacity & Resilience



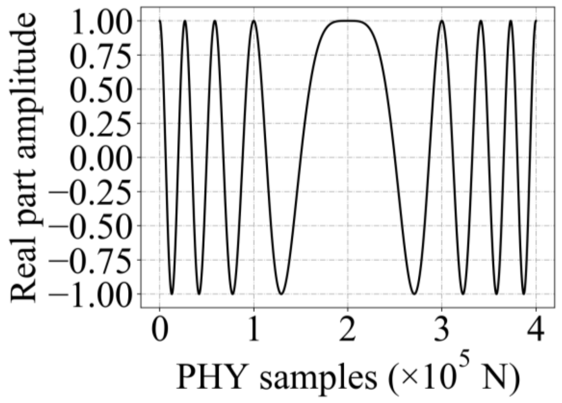
- The noise resilience of LoRa is **sufficient** when at short distances which has strong channel quality.
- Is it possible to use covert channel to explore the **trade-off** between the covert channel's capacity and legitimate channel's resilience?

Core Idea: CSS on Amplitude for Covert Channel

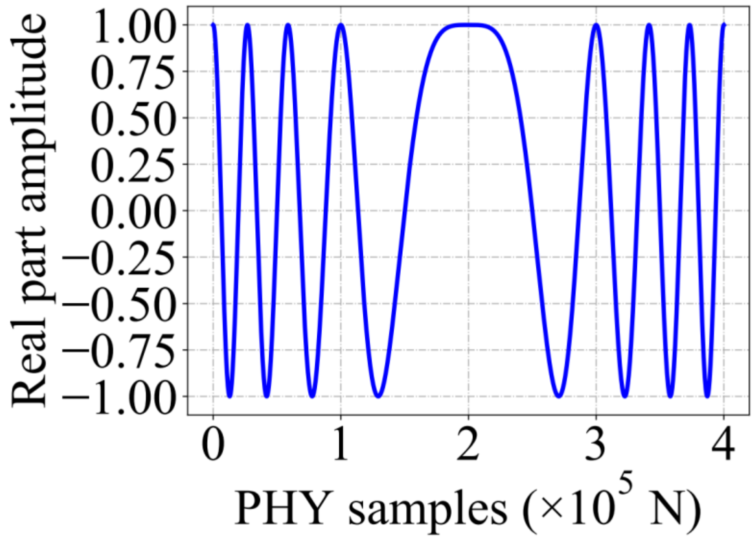


Amplitude **without** covert channel

Embed the **waveform** of the real part of the chirp to the amplitude



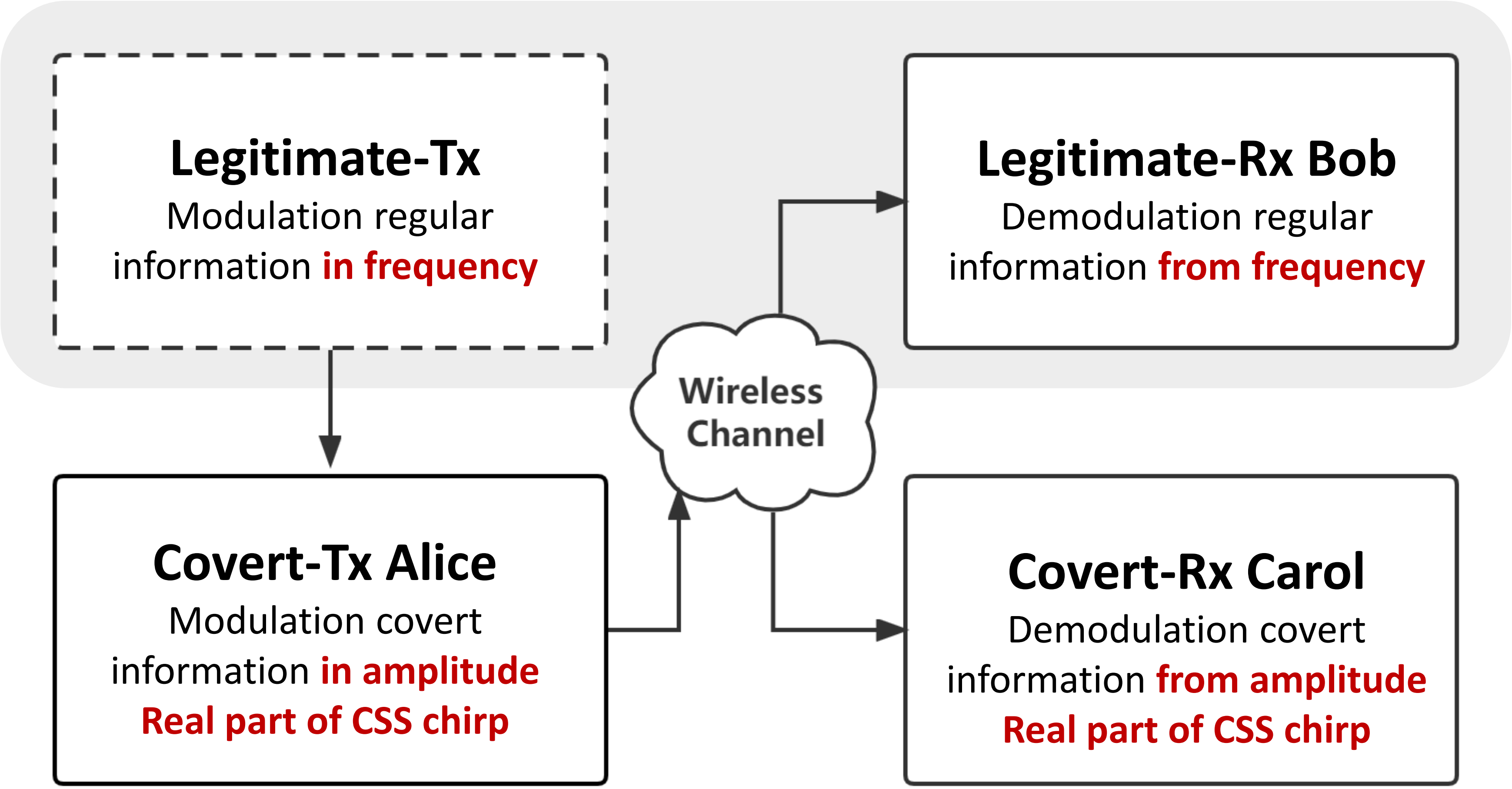
Covert Channel Chirp



Amplitude **with** covert channel

- Our core idea is to use **CSS modulation on the amplitude** of signal to build a **long-range and noise resilient** covert channel.

Design-Workflow



Legitimate Channel LoRa Chirp

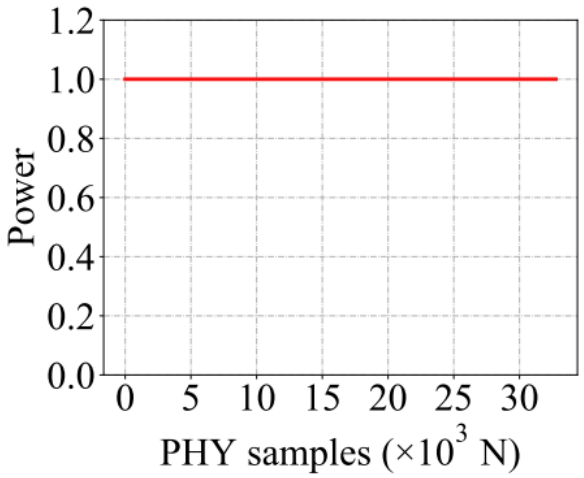
Covert Channel LoPhy Chirp

Challenges

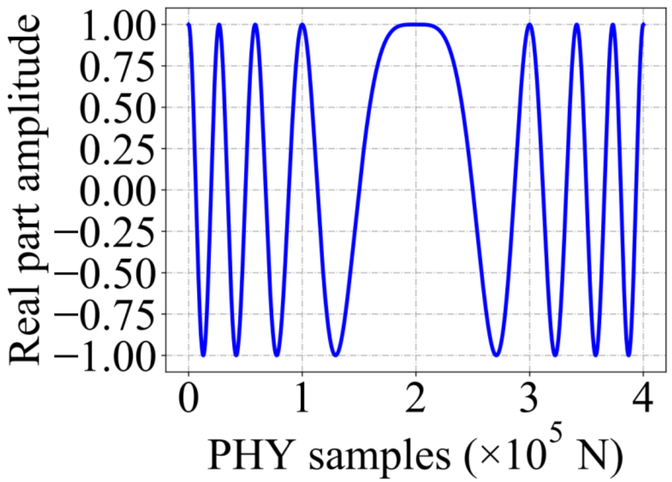
- **The absence of the imaginary part**
- The information loss and impact on legitimate channel
- The compatibility with COTS LoRa end devices

Challenge-1: Imaginary Part Absence

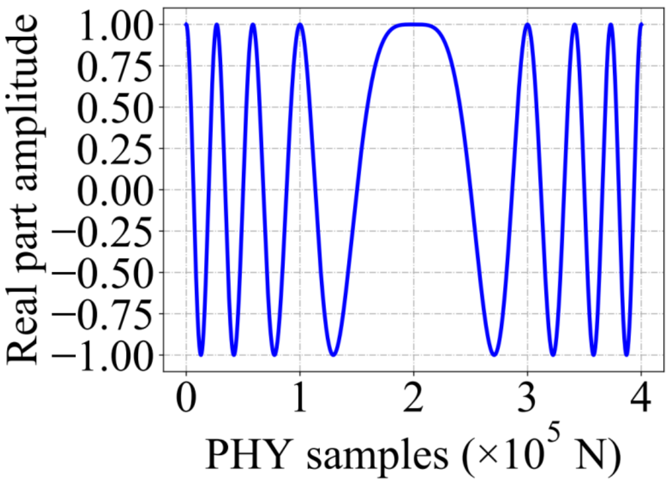
- **Transmitter:**



Real Part Embedding

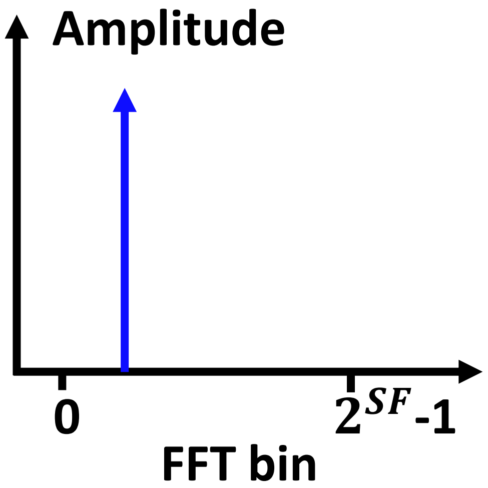


- **Receiver:**



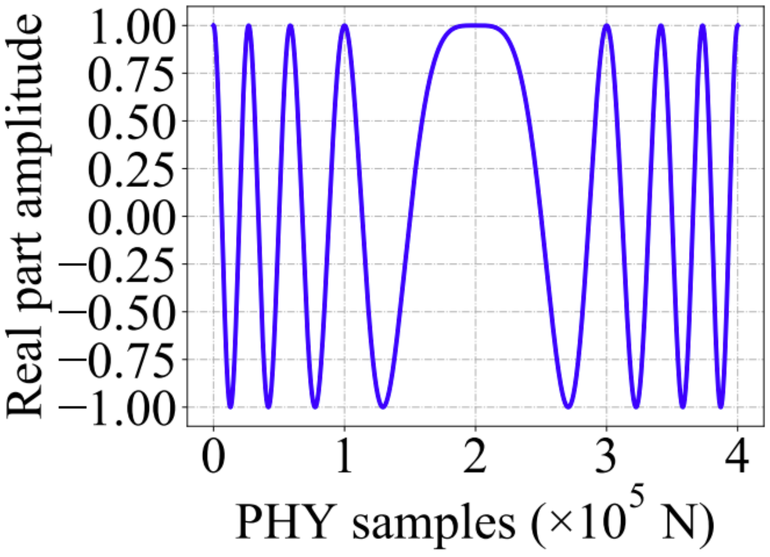
?

Missing Imag Part



Solution-1: Imaginary Part Generation

Real part / I value

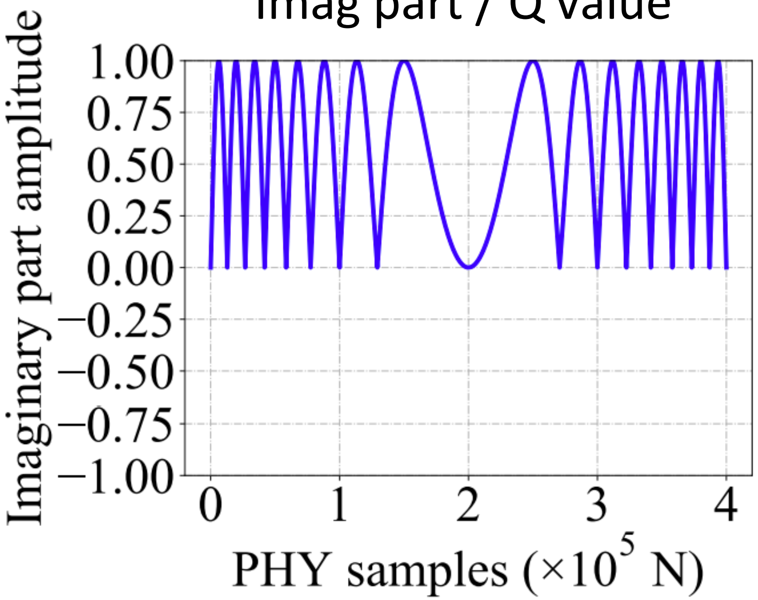


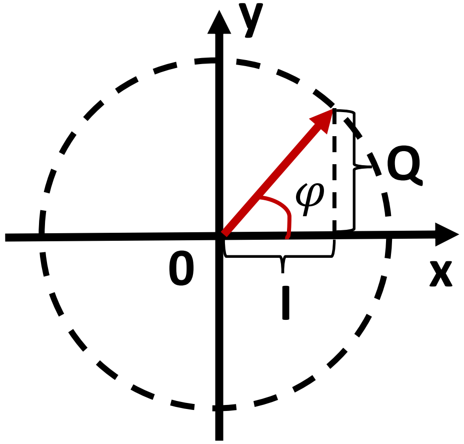
Imaginary part generation

$$\because \underbrace{\cos\varphi}_{I} + \underbrace{\sin\varphi}_{Q} \cdot j = C$$

$$\therefore I_{\varphi\, c}(t) = \sin \underbrace{\left\{\arccos\left[R_{\varphi\, c}(t)\right]\right\}}_{\varphi}$$

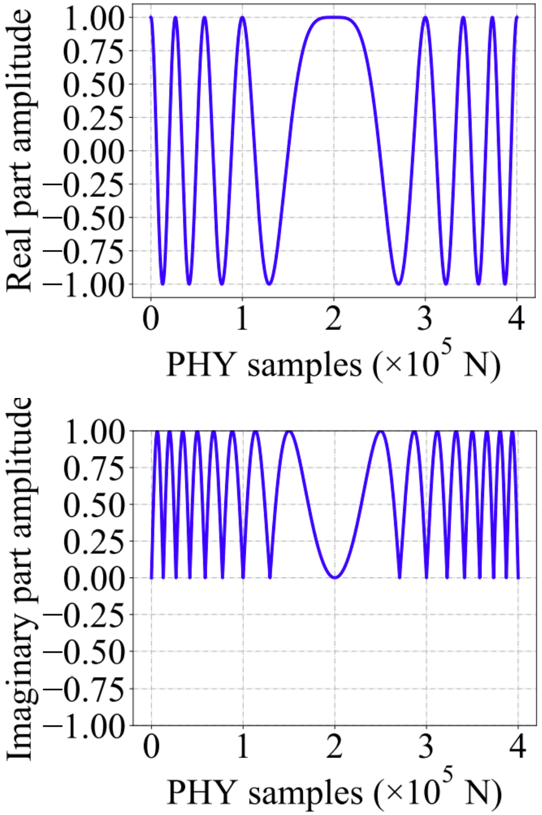
Imag part / Q value



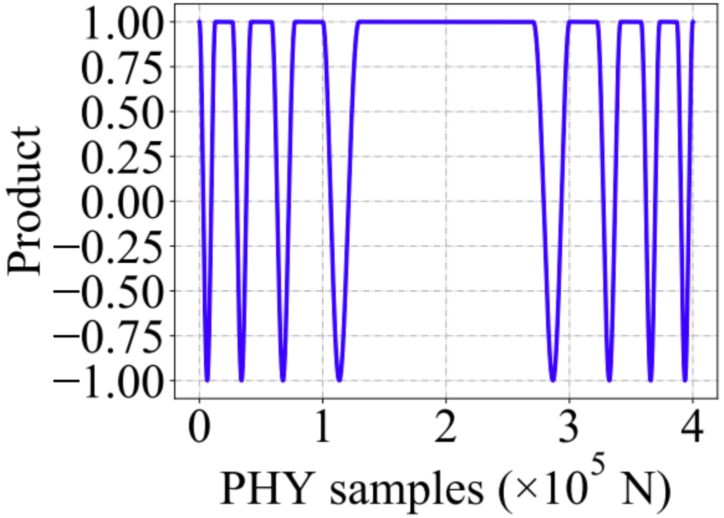


Solution-1: Imaginary Part Generation

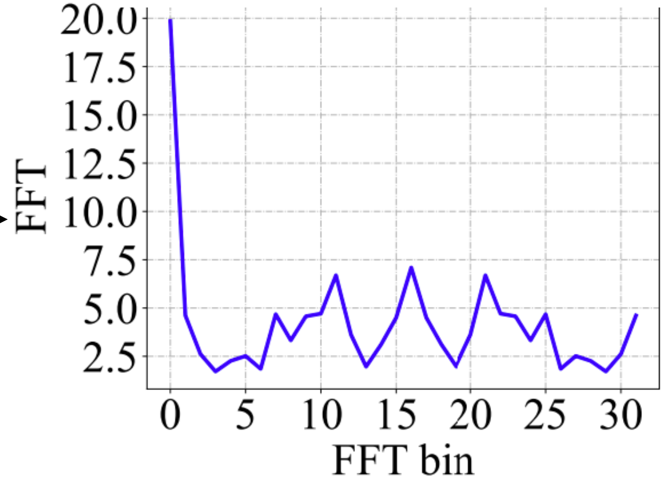
Covert LoPhy Chirp



Dechirping

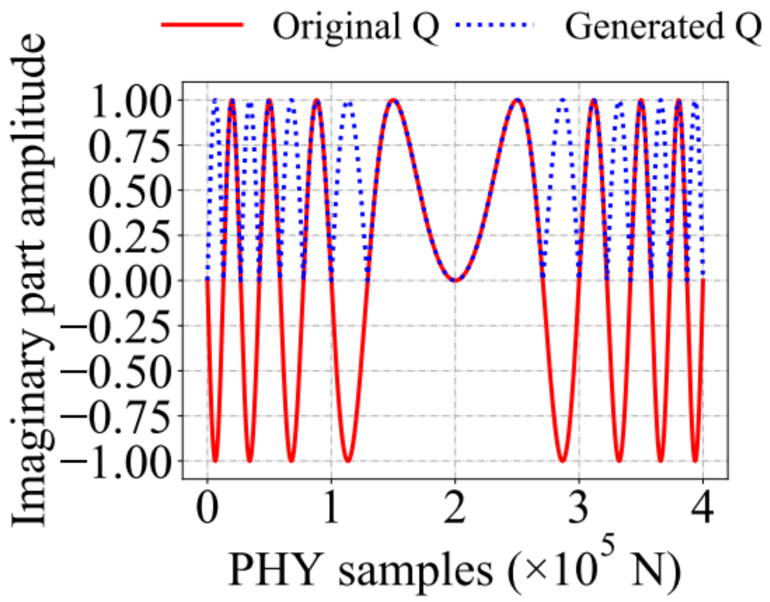


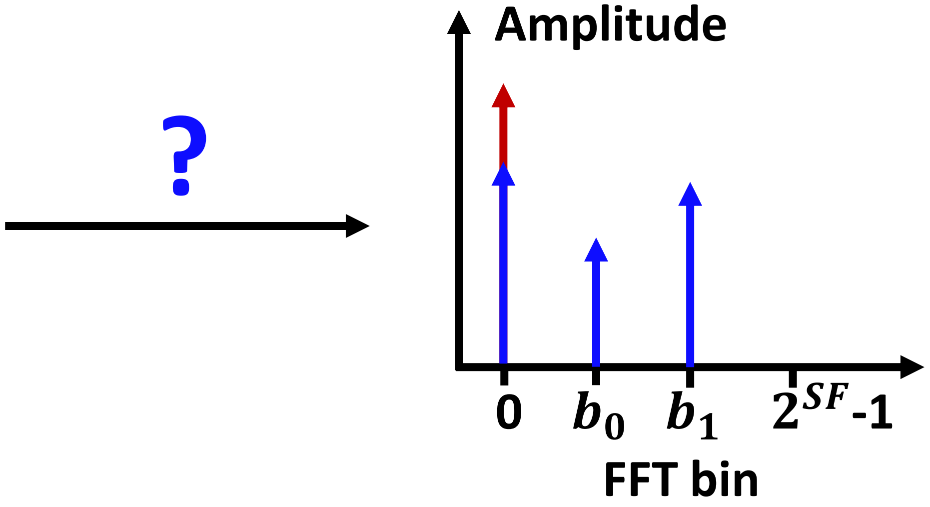
FFT



- We **multiply it with a covert standard down-chirp** $C_{0c}^{*}(t)$ and recover $f_{\varphi c}$ by locating **the peak in an FFT** of the de-chirped symbol, just like the standard CSS demodulation.

Phase Information Loss





Phase information loss

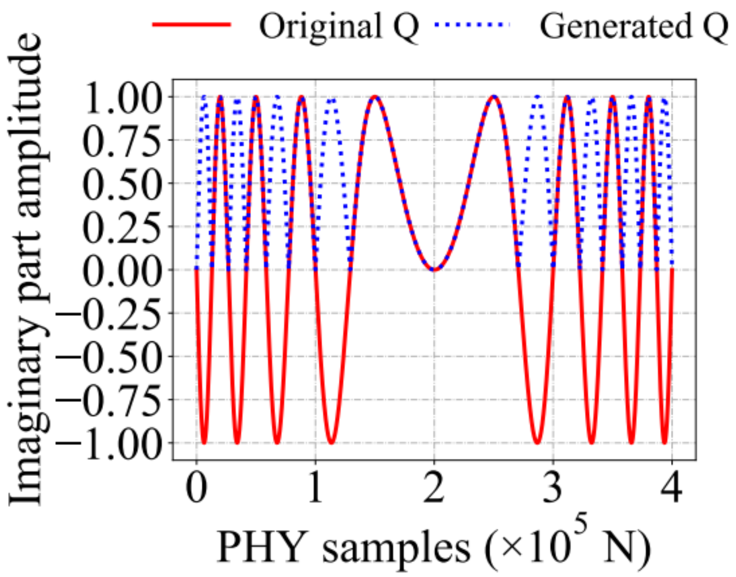
Decoding accuracy?

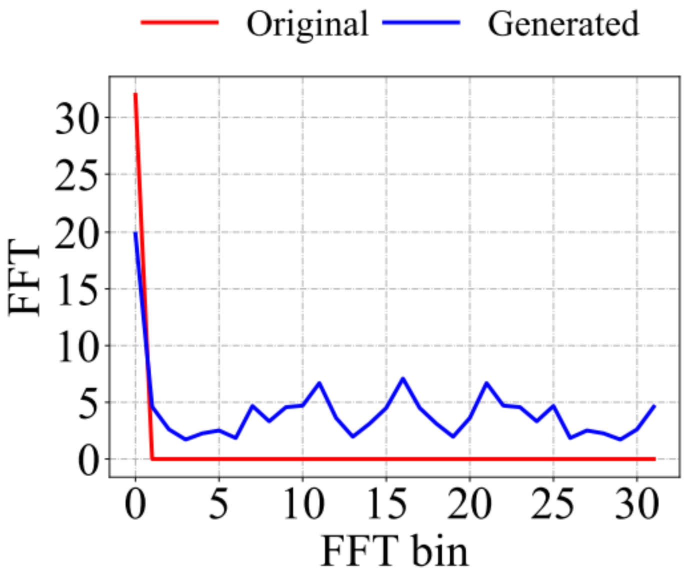
Noise resilience?

Challenges

- ✓ The absence of the imaginary part
- ➢ **The information loss and impact on legitimate channel**
- ➢ The compatibility with COTS LoRa end devices

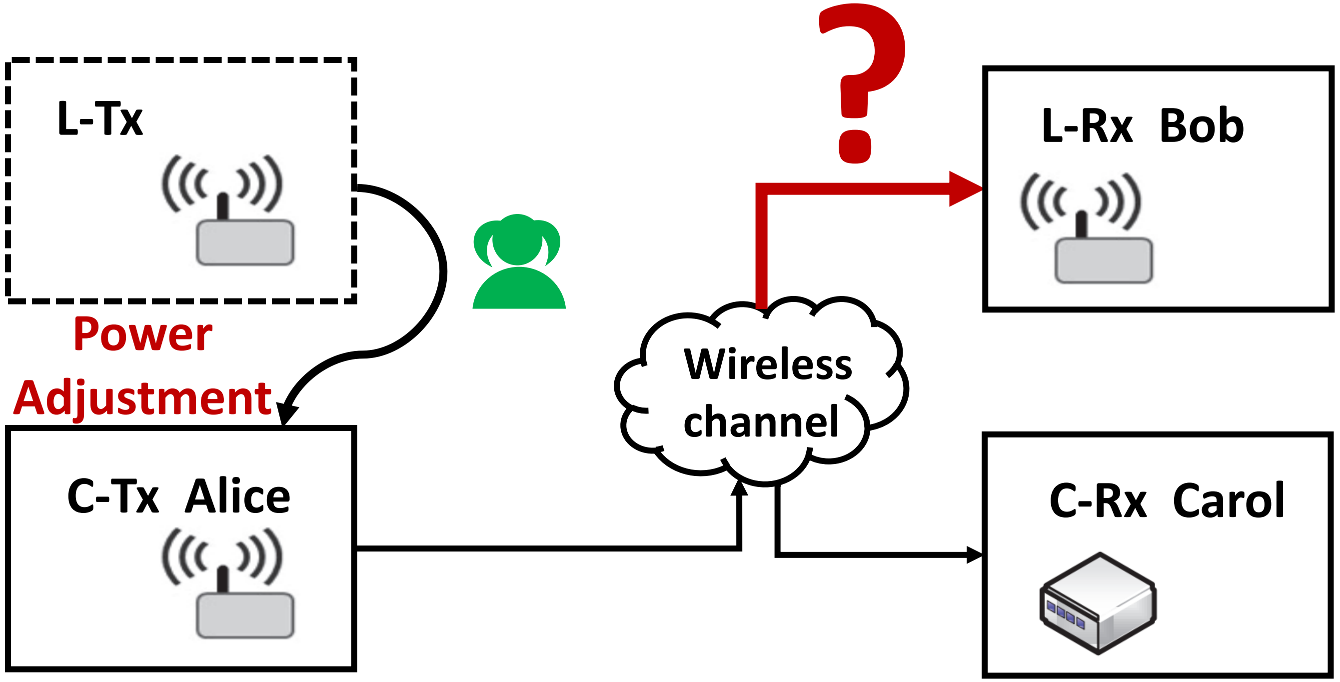
Solution-2: Impact of Information Loss





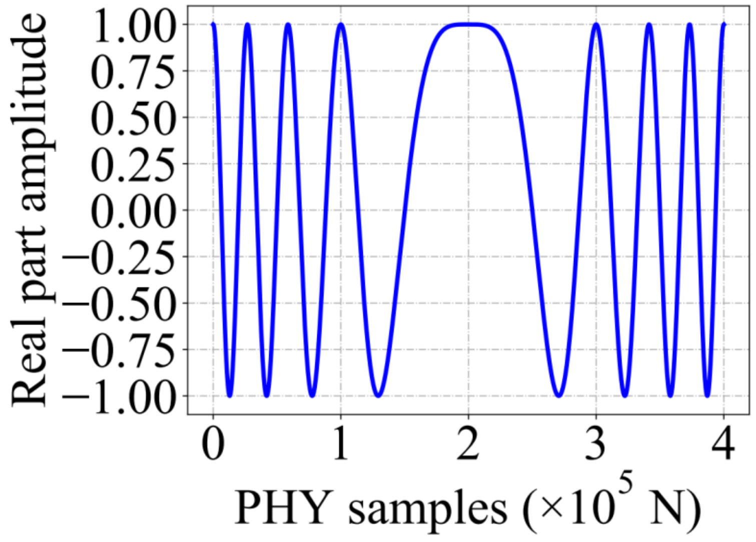
- The FFT peak of the generated one is **lower than** the original one.
- It falls into **the same FFT bin** as the original one.
- The frequency information still remains.
- The generated one can still gain the noise resilience and the receiver can still demodulate the information correctly.

Impact on Legitimate Channel

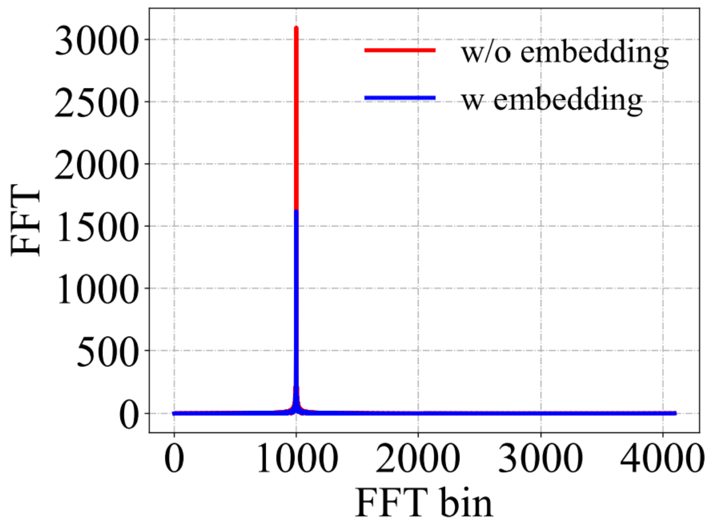


Will the covert channel affect the transmission of legitimate channel?

Solution-2: Impact on Legitimate Channel



Signal Power Attenuation

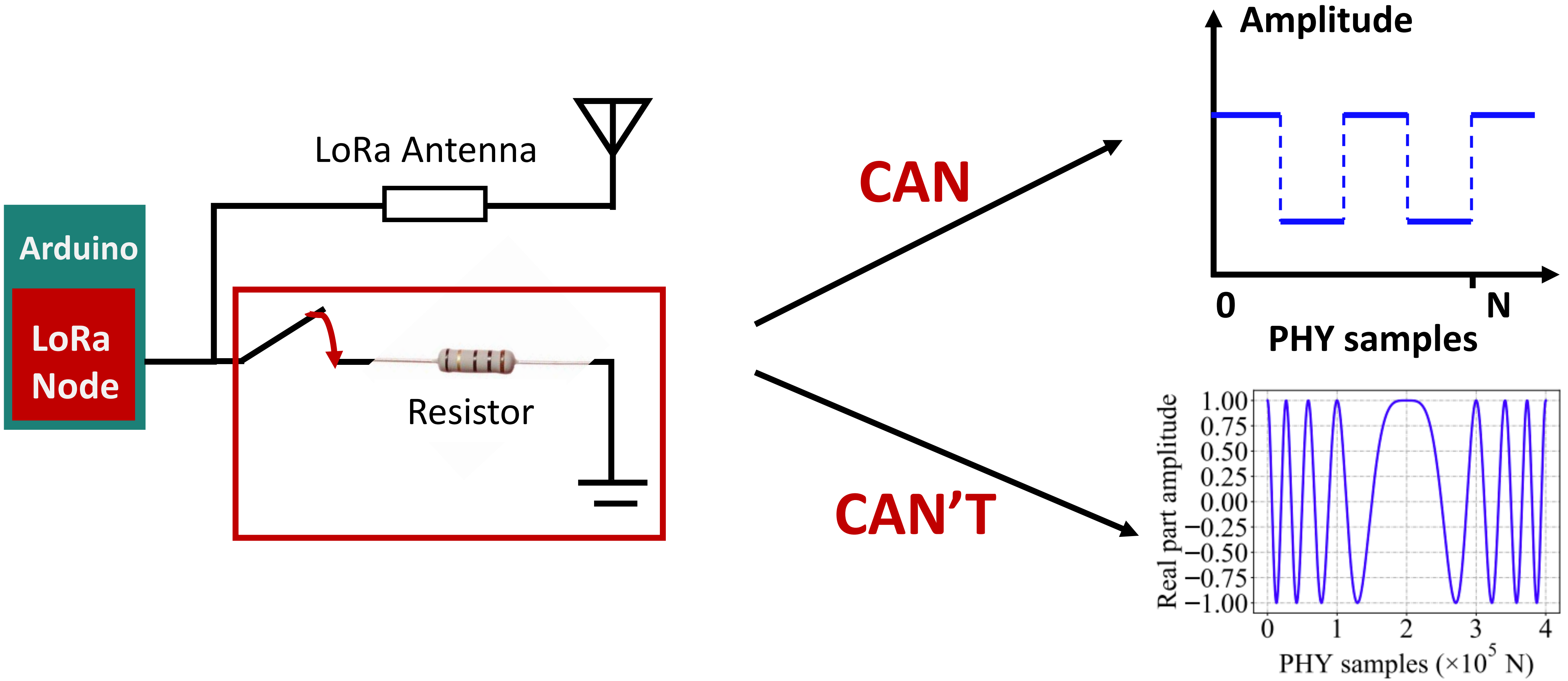


- The amplitude of the FFT peak after embedding is **lower than** the original one.
- The peak still **stands out** and still **gains noise resilience**.
- It proves to be unaffected on the final symbol determination of legitimate channel when at short distances.

Challenges

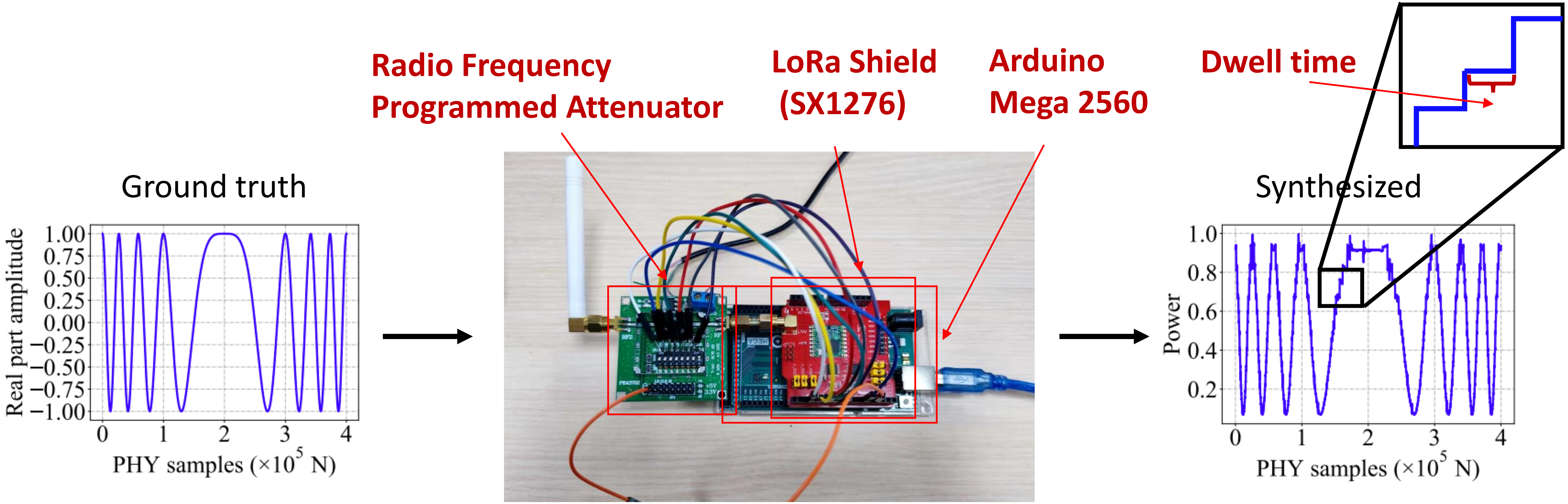
- ✓ The absence of the imaginary part
- ✓ The information loss and impact on legitimate channel
- ➢ **The compatibility with COTS LoRa end devices**

Solution-3: A Natural Idea



Amplitude Variations

Solution-3: Compatibility with COTS LoRa

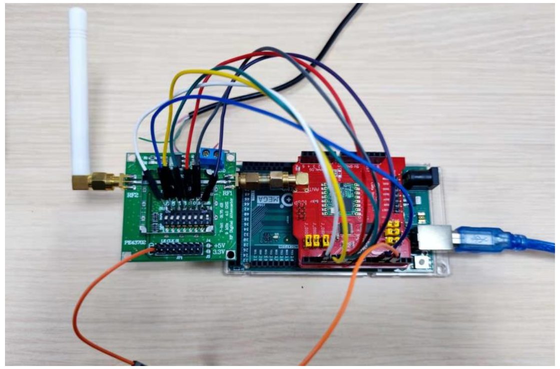


- LoPhy addresses this issue using attenuator ($20) by controlling it to **approximate a covert chirp** as a sequence of discrete amplitude levels.

Evaluation-Setups

Tx

Legitimate & Covert Tx



- Arduino
- SX1276
- Radio Frequency Programmed Attenuator ($20)

Rx

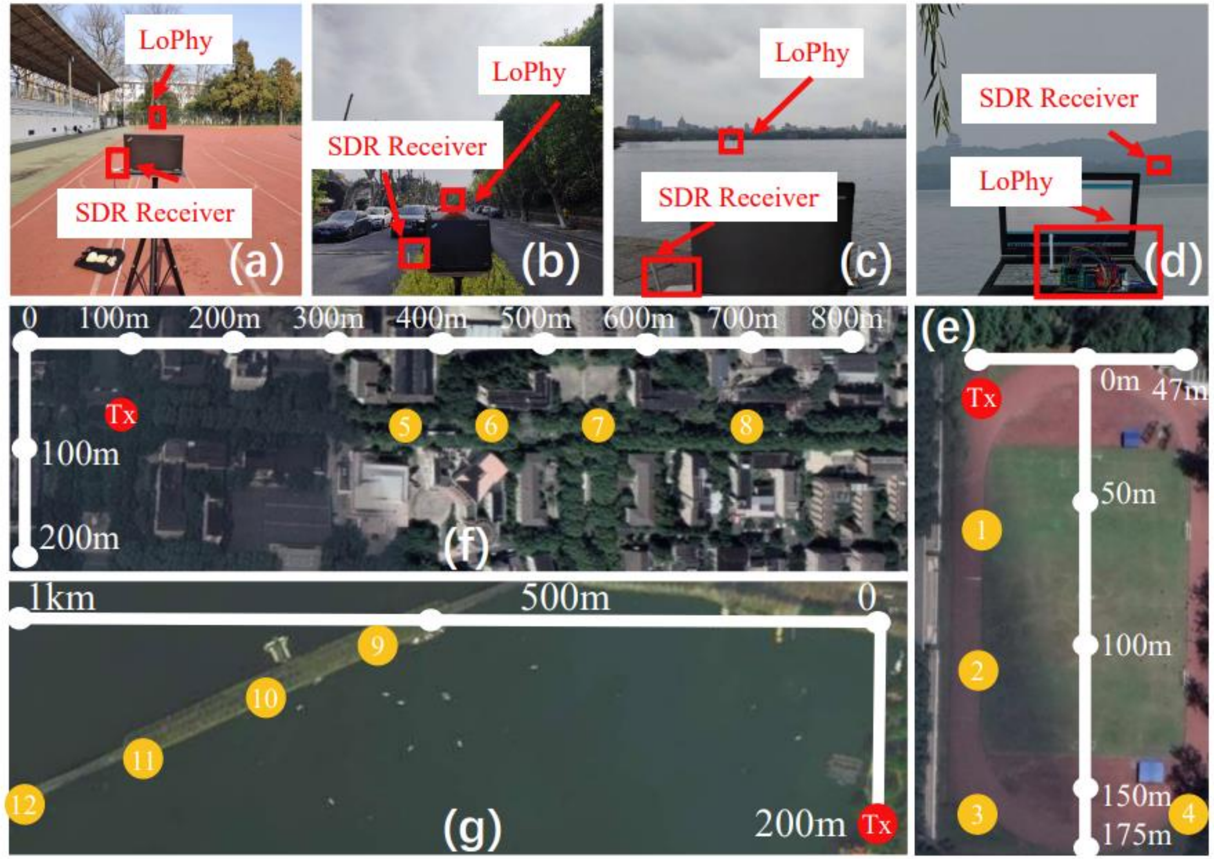
Covert Rx

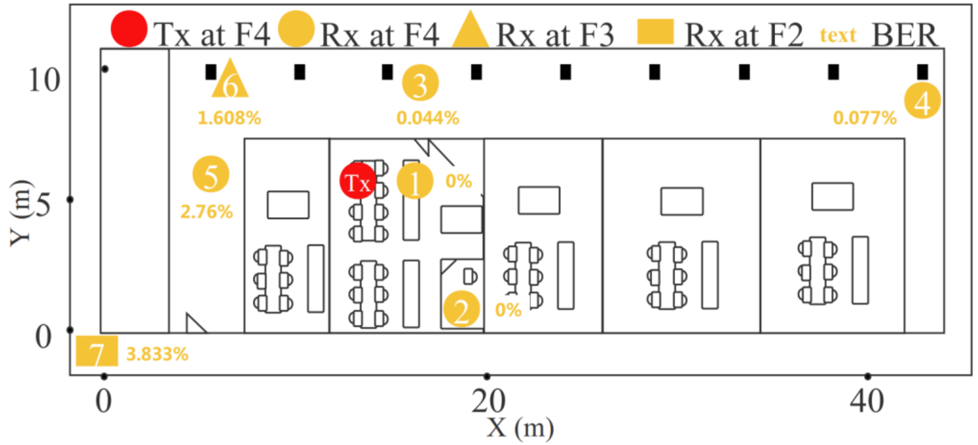
- RTL-SDR dongle ($25)

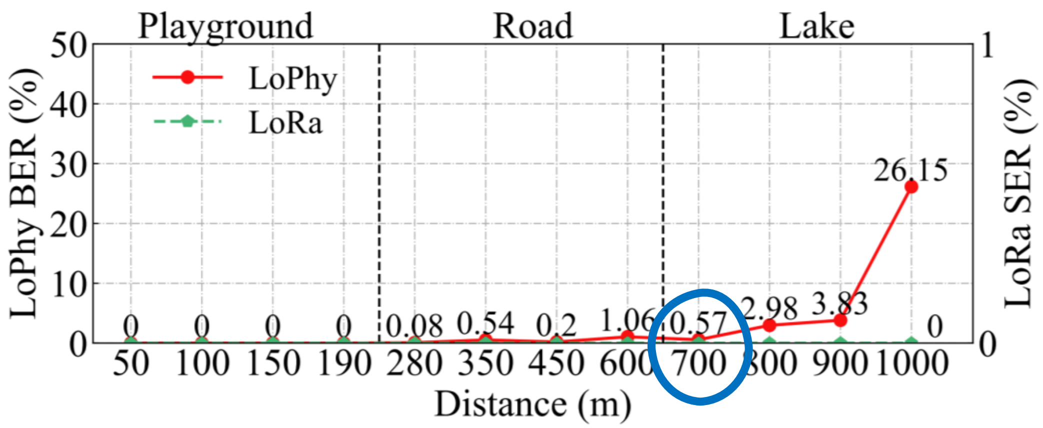
Legitimate Rx

- COTS LoRa Node

Evaluation-Indoor and Outdoor Experiments

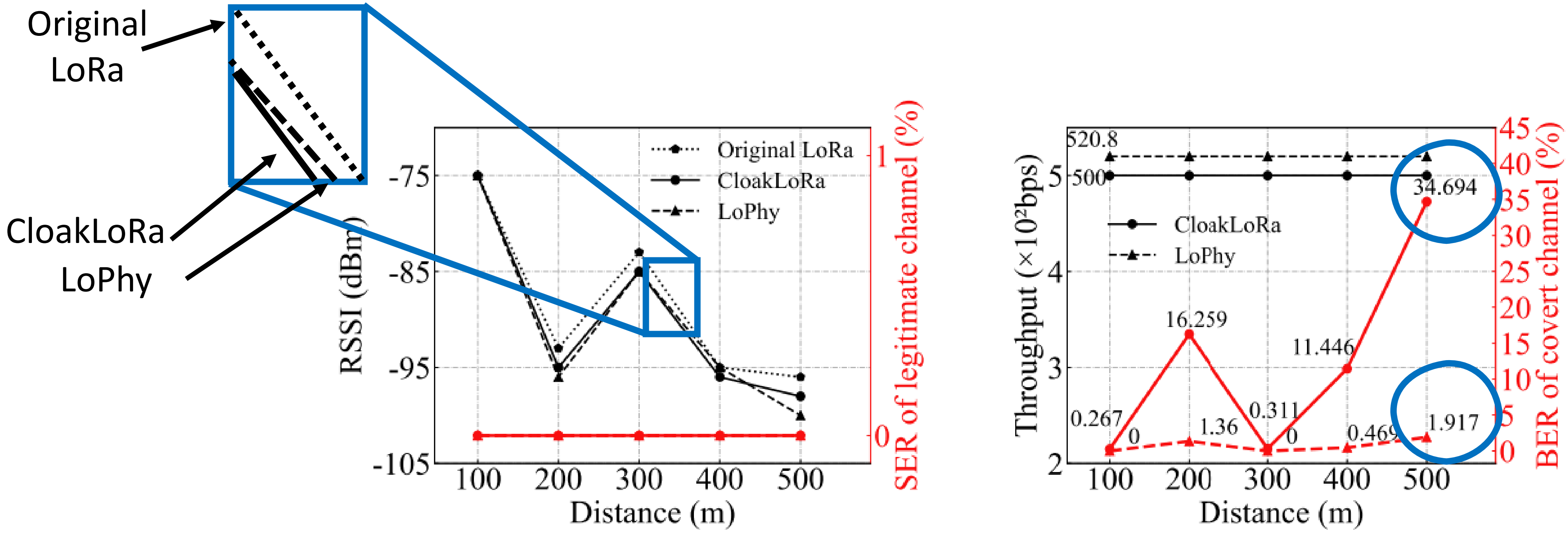






- The BER of the covert channel achieves **0.57% at 700m**.
- The SER of the legitimate LoRa remains **0%** at each location.
- LoPhy **does not affect** the legitimate channel transmission in all experiments.

Evaluation-Comparison Experiments



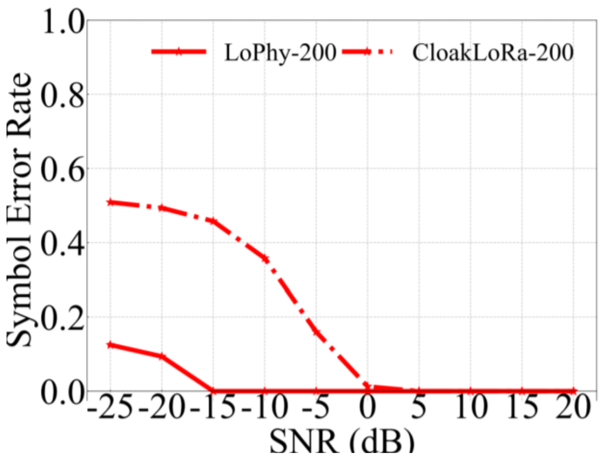
(a) Impact on legitimate channel

(b) Performance of covert channel

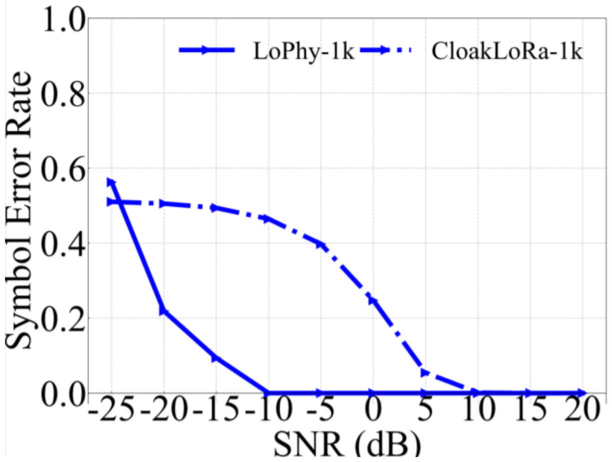
- Both the two weaken the RSSI but **do not affect** the SER of legitimate channel.
- *LoPhy* has **a lower BER at every distance** compared with *CloakLoRa.*
- *LoPhy* significantly **improves the noise resilience** compared with *CloakLoRa*.

Evaluation-Comparison Simulations

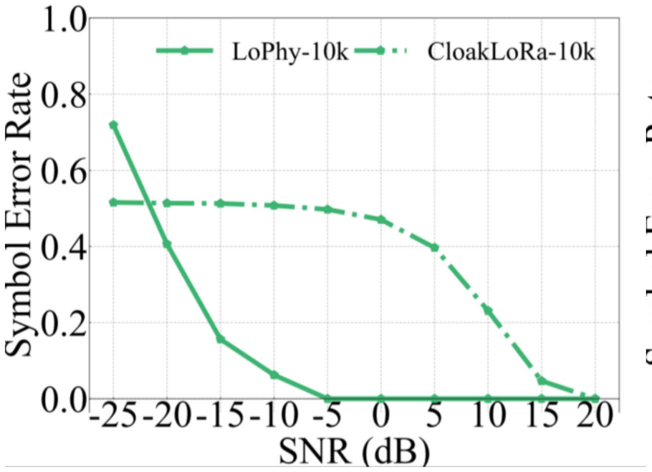
Throughput=200bps



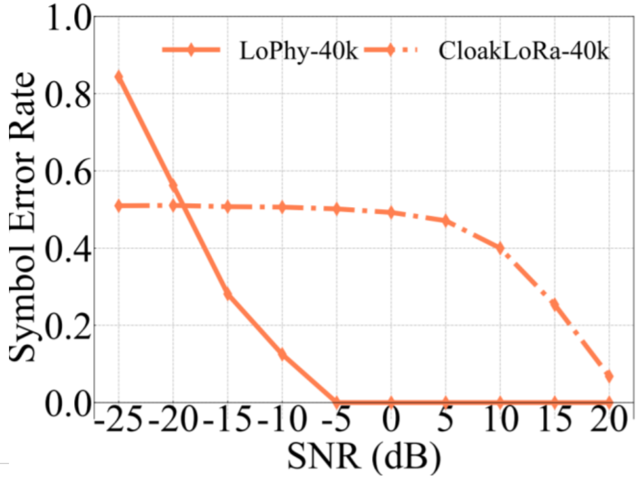
Throughput=1kbps



Throughput=10kbps



Throughput=40kbps



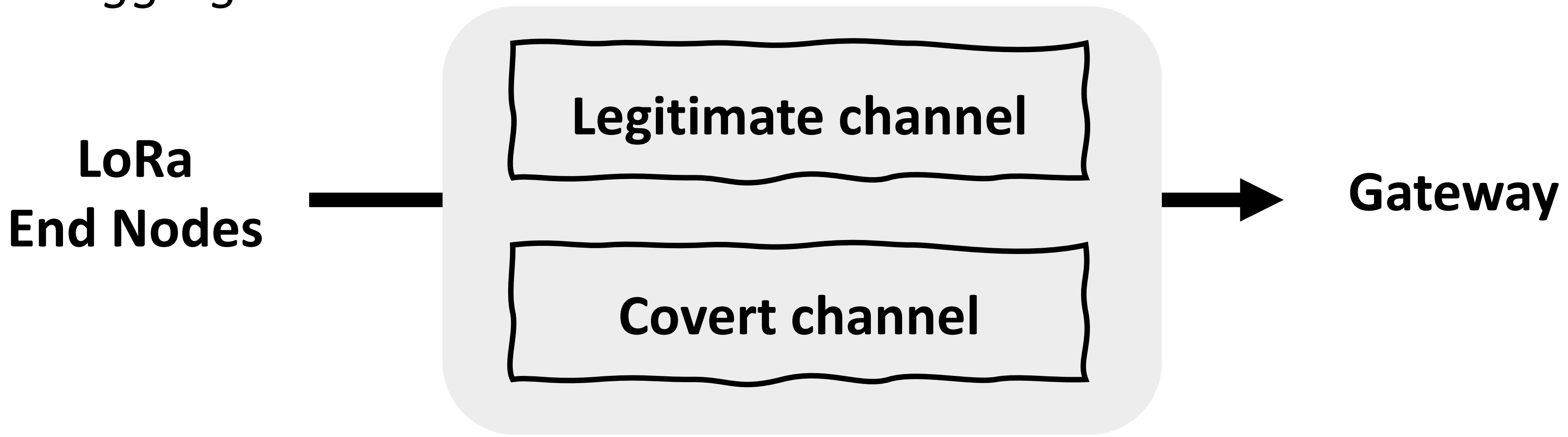
LoPhy symbol number $=2^{SF} = 2^5 = 32$

LoRa symbol number = 2

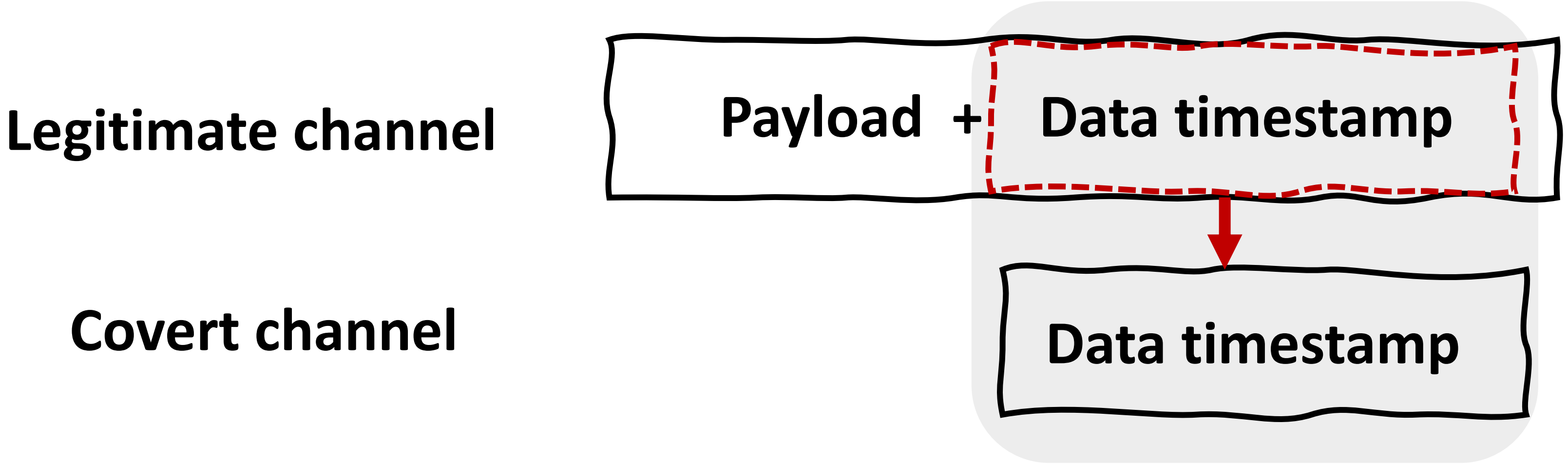
- *LoPhy* **maintains 0%** SER when SNR is higher than −5 dB at all throughput.
- *CloakLoRa* **cannot maintain a low SER** when SNR is lower than 0 dB even the bit rate is lowered to 200 bps.
- LoPhy has about **63×** $(\mathbf{10^{\frac{3}{10}}/10^{\frac{-15}{10}}})$ gain on noise resilience by calculating the SNR under which they reach 0% SER.

Applications

- *Channel Aggregation*



- *Data Timestamping*



Conclusion

- 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.

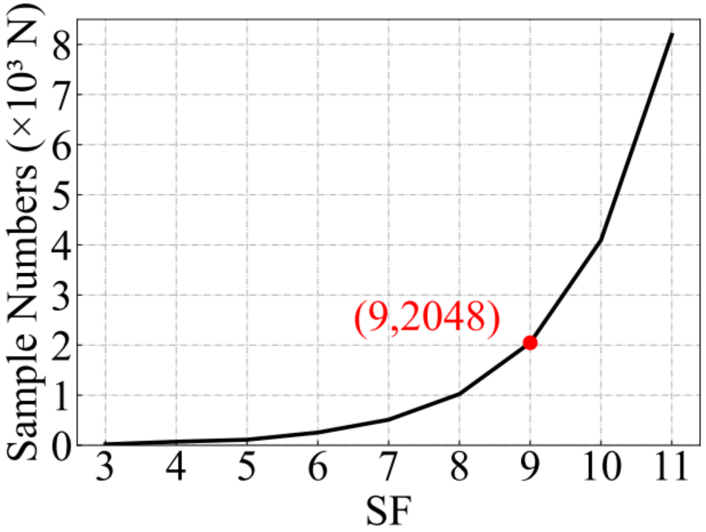
- We present **two new applications** enabled by LoPhy, which help improve the throughput and save energy of the legitimate channel.

More details: 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, 13 pages.

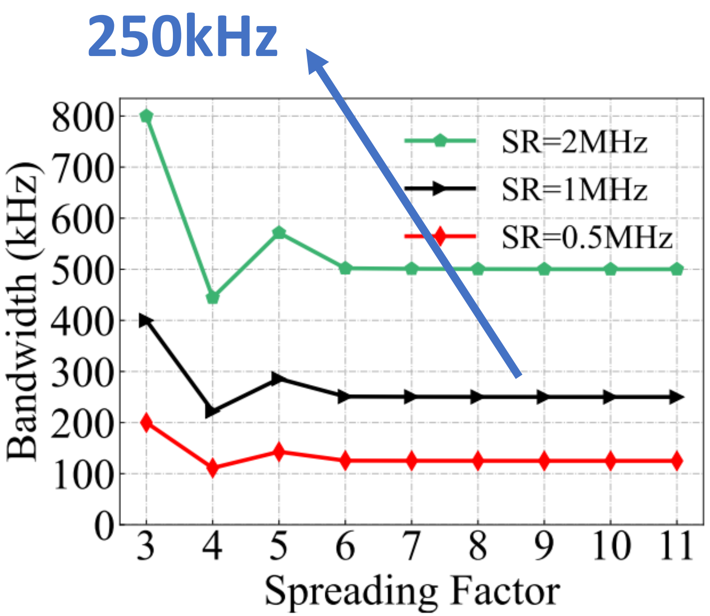
Thank you!
(Q&A)

浙江大学
ZHEJIANG UNIVERSITY

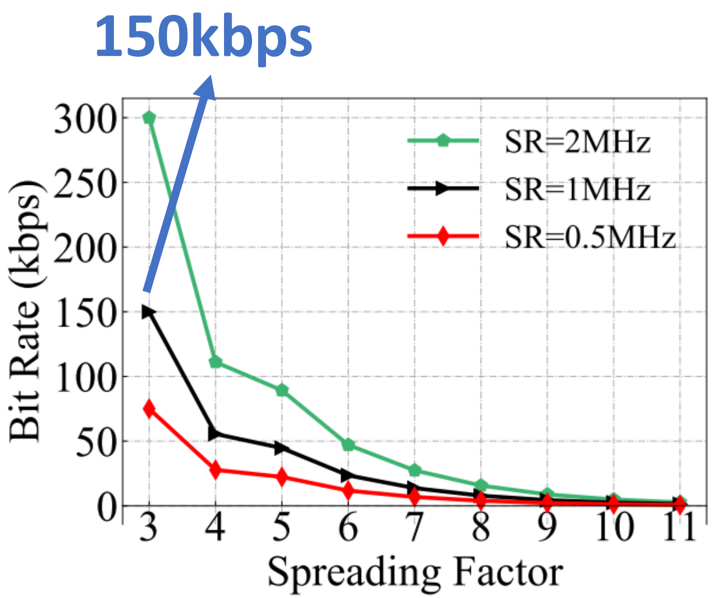
Numerical Study



(b) Minimum sample-per-symbol



(c) Maximum bandwidth



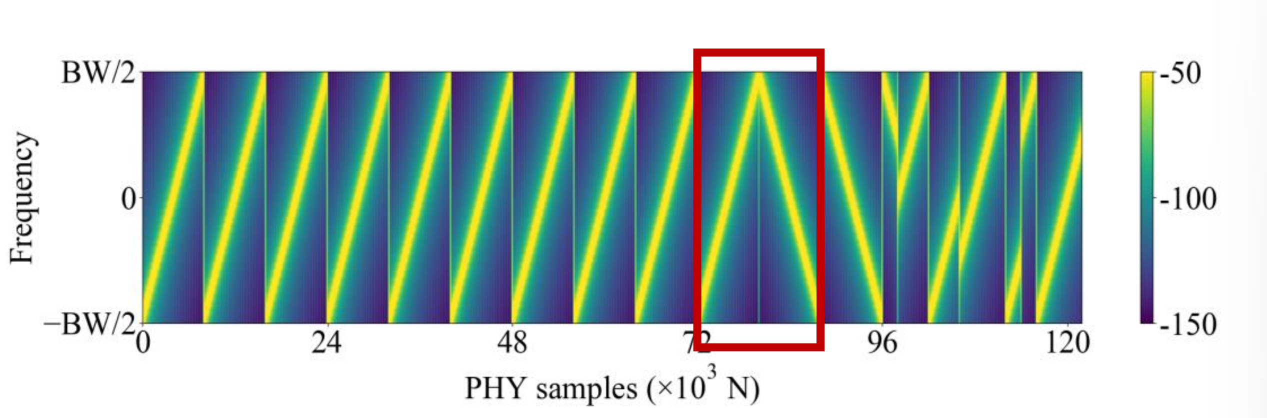
(d) Maximum bit rate

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

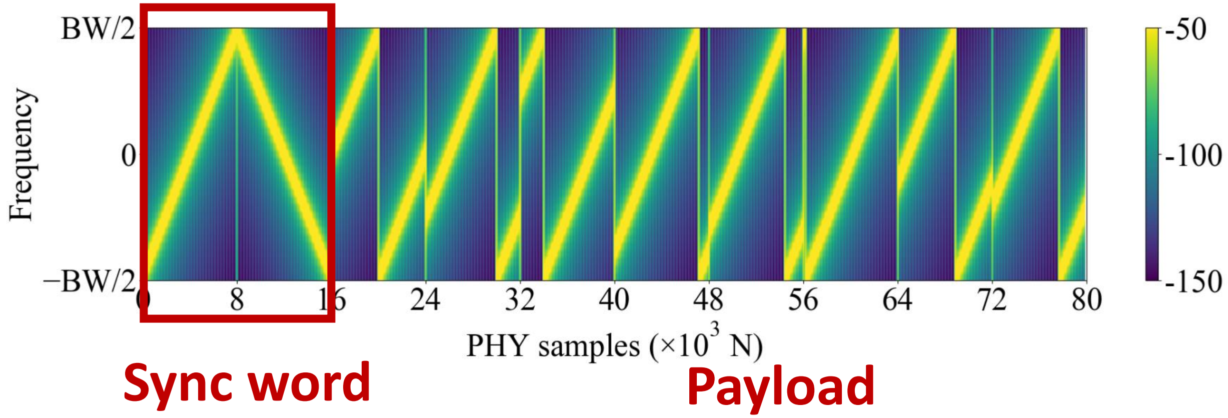
$$bit\ rate = \frac{SF_c}{T_{sc}} = \frac{SF_c}{\left(\frac{2^{SF_c}}{BW_c}\right)} = BW_c \cdot \frac{SF_c}{2^{SF_c}}$$

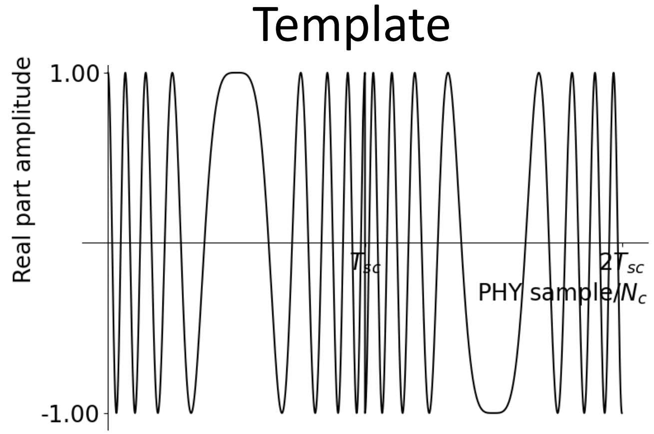
Design-Detection

- Legitimate LoRa frame detection



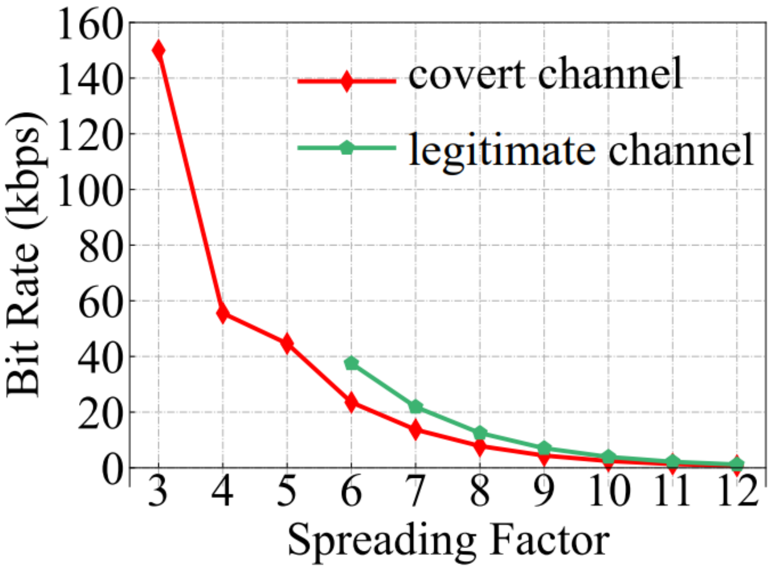
- Covert LoPhy frame detection



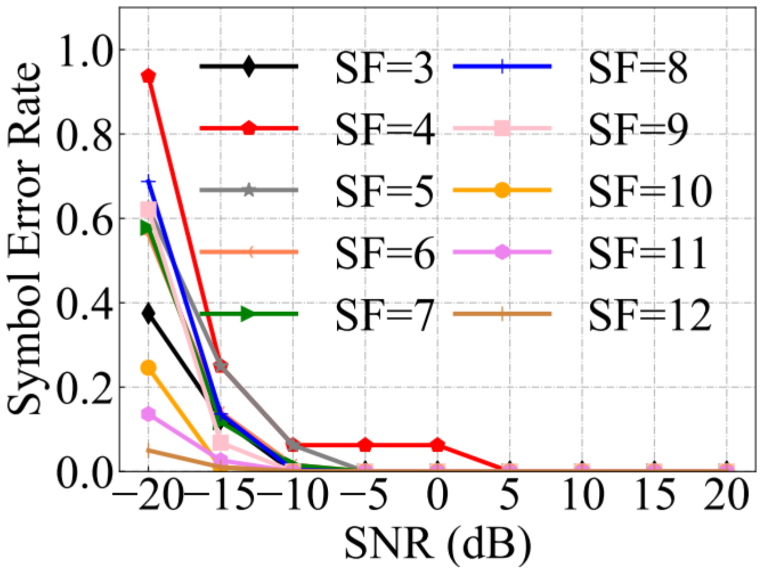


- We set up-chirp and the opposite number of down-chirp as LoRa **sync word** to help locate the packet's symbol boundary positions.
- We slide the sync word template **sample by sample** to find the exact sample point.

Numerical Study



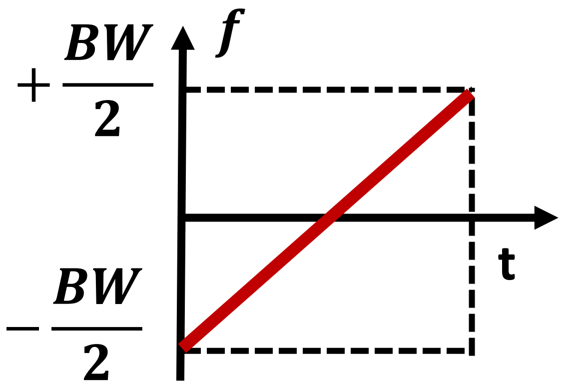
(a) Bit rate of different channels.



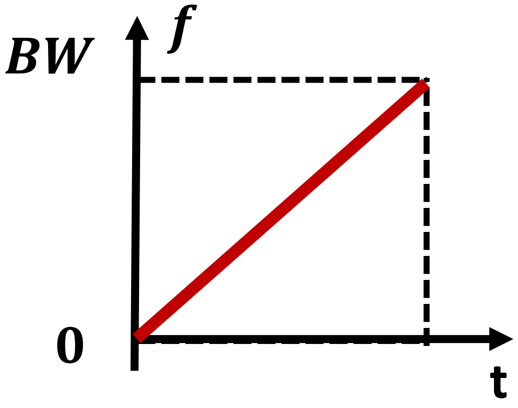
(b) SER of the covert channel.

Solution-1: Imaginary Part Generation

LoRa: Double-sideband (DSB)



Sound: Single-sideband (SSB)



- We can not apply **Hilbert Transform** to obtain the imaginary part like the SSB signals.