Demo Abstract: CLoRa-A Covert Channel over LoRa PHY

Ningning Hou
The Hong Kong Polytechnic University
Hong Kong, China
csnhou@comp.polyu.edu.hk

Yuanqing Zheng
The Hong Kong Polytechnic University
Hong Kong, China
yqzheng@comp.polyu.edu.hk

***Abstract*—LoRa adopts a unique modulation scheme (chirp spread spectrum (CSS)) to enable long range communication at low power consumption. CSS uses the initial frequencies of LoRa chirps to differentiate LoRa symbols, while simply ignoring other RF parameters (*e.g.*, amplitude and phase). Driven by this observation, we build a covert channel (named `CLoRa`) by embedding covert information with a modulation scheme orthogonal to CSS. We implement `CLoRa` with a COTS LoRa node (Tx) and a low-cost receive-only SDR dongle (Rx). The experiment results show that `CLoRa` can send covert information over 250 m. This demo reveals that the LoRa physical layer leaves sufficient room to build a covert channel by embedding covert information with a modulation scheme orthogonal to CSS.**

I. Introduction

The security of IoT devices is important to support the wide adoption of LoRa technology. Current LoRa security mechanisms mainly use message encryption to ensure end-to-end communication. For example, LoRaWAN uses AES encryption at the upper layer. However, the upper layer security mechanisms do not examine physical layer parameters (*e.g.*, amplitude, phase, and waveform), which leaves the LoRa PHY vulnerable to attacks. We ask the question that *would it be possible for attackers to build a covert channel over LoRa PHY?* Consider a smart home scenario (as shown in Fig. 1), LoRa-enabled IoT sensors (transmitter Alice, *e.g.*, smart meters for electricity, water, gas, or smart door lock, etc.) can be compromised by an attacker modulating the neglected PHY parameters (*e.g.*, amplitude) to secretly send covert information. As such, the compromised transmitter can 1) secretly transmit sensory data to the attacker (covert receiver Carol) 2) without affecting the normal communication to legitimate gateway receiver (legitimate LoRa receiver Bob) and 3) avoid being detected by security mechanism (warden Willie). The attacker may infer sensitive information about the residents from these data. For example, the daily routine of the residents (such as the time of home leaving/arriving) can be inferred. This example raises security risks and privacy concerns of building a covert channel over LoRa PHY.

In this demo, we design and implement `CLoRa` to demonstrate the feasibility of building a covert channel. We prototype covert transmitter use COTS LoRa nodes with passive components and covert receiver with low-cost receive-only SDR dongle. The key idea of `CLoRa` is to leverage amplitude modulation (AM) to embed covert information. Since AM is orthogonal to CSS modulation, we can modulate the amplitude

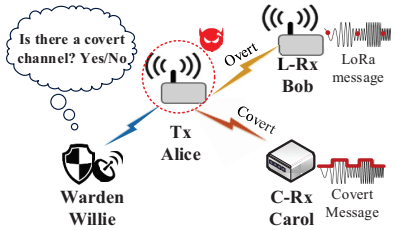
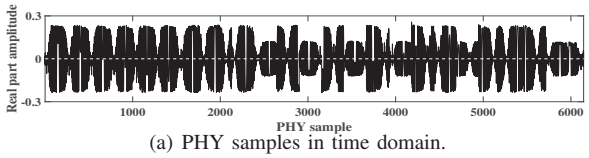
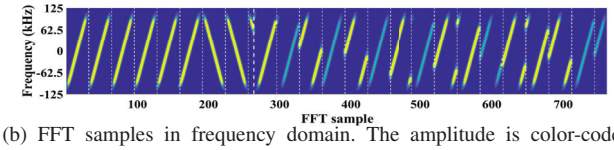


Fig. 1: Covert communication scenario.



(a) PHY samples in time domain.



(b) FFT samples in frequency domain. The amplitude is color-coded. Light color indicates high power, while dark color indicates low power.

Fig. 2: Covert channel signals captured by a software defined radio. The amplitude of chirps are modulated to carry covert information.

of LoRa chirps without affecting the normal LoRa communication. As a result, AM modulated LoRa chirps carry both original CSS and AM covert information. Bob, the legitimate receiver, can demodulate the original CSS information as the frequencies of LoRa chirps are unchanged. And the covert receiver, Carol, can focus on the variation of received signal strength and extract the embedded covert information. To the best of our knowledge, we are the first to reveal the vulnerability and demonstrate the feasibility of building a covert channel over LoRa PHY. We find that LoRa leaves sufficient room in PHY for attackers to build a covert channel, which may impede the wide deployment of IoT applications and is largely overlooked by current security mechanisms.

II. Design and Implementation

To test the feasibility, we first conduct a proof-of-concept based on GNU Radio and GR-LoRa projects [1], [2]. Fig. 2 shows the AM modulated LoRa chirps in both time domain and frequency domain. We can observe alternating patterns of the amplitude in the payload chirps. The signal strength is color coded in Fig. 2(b), *i.e.*, brighter color indicates stronger

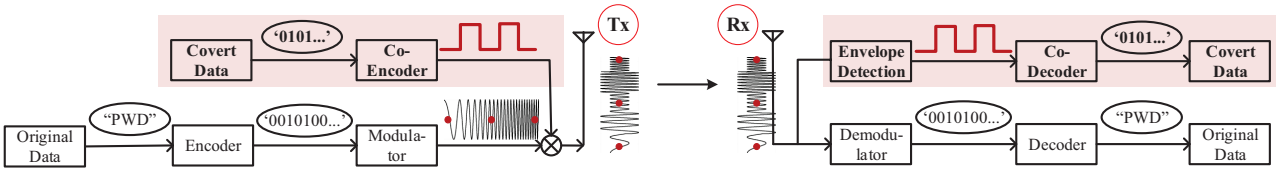


Fig. 3: Workflow of covert channel transmitter and receiver..

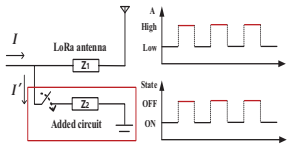


Fig. 4: Circuit Design.

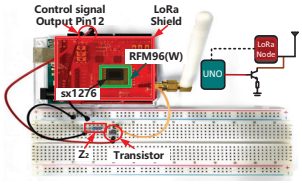


Fig. 5: Hardware implementation of covert Tx.

signal strength. If Alice uses chirp with low power to indicate bit '0' and high power to indicate bit '1', a series of covert bits (*i.e.*,'1010101011...' in this example) can be embedded and Carol can use an envelope detector to decode the covert information. As the initial frequency of chirps remains unchanged, Bob can still decode the payload even though the amplitude of chirps has been intentionally modulated. The workflow of `CLoRa` is shown in Fig. 3. At the transmitter side, we add AM components which can modulate the amplitude of LoRa chirps and thus embed covert information. At the covert receiver side, we focus on covert information extraction because we do not need to decode LoRa message. As the covert information is embedded in the variation of the amplitude, the covert information extraction process essentially implements the AM demodulation process.

We then implement a hardware prototype of TX with COTS LoRa node. Fig. 4 shows the simplified circuit design. We add a new branch (consisting of a switch and an impedance Z_2) to control the amplitude of LoRa chirps. When the state of the switch is OFF, the current (denoted as I) flows via Z_1 and the antenna, as if there is no external circuit. When the state of the switch is ON, as a portion of current is leaked through the added circuit (denoted as I'), the current flows through the antenna load becomes $I - I'$. As such, the RF power of the outgoing signals become lower when the switch is ON, and become higher when the switch is OFF. As a result, by altering the state of the switch, we can generate changing amplitudes.

Fig. 5 shows the corresponding hardware implementation. The AM circuit only consists of a transistor and a resistor. The transistor is used as a switch to control the ON/OFF state transition, while the resistor plays the role of the impedance Z_2 in Fig. 4. We use an Arduino UNO to control the switch. The Arduino board outputs high (*i.e.*, 5 V) or low (*i.e.*, 0 V) to alter the states of the transistor and thereby modulates the amplitude of LoRa chirps. In practice, the IoT devices can be compromised by attackers before/after delivering to users as reported in previous works [3].

III. Preliminary Results

Feasibility. We further conduct experiment with our hardware prototype. We configure the bit duration of output pin (*i.e.*, pin 12 in Fig. 5) to be 5 ms (*i.e.*, 200 bps), while each LoRa chirp takes approximately 1 ms ($T = SF^2/BW \approx 1$ ms, when $SF = 8$ and $BW = 250K$). By plotting the received PHY sample, we observe that every 5 chirps share the same power level alternatively which is consists with the modulation at covert transmitter. We use another COTS LoRa node as legitimate receiver and it decodes the regular LoRa message correctly. In summary, both the SDR based proof-of-concept and hardware prototype experiments demonstrate that we can build a covert channel over LoRa PHY by alternating the amplitudes of LoRa chirps. In particular, 1) Bob can successfully decode the payload of LoRa and 2) Alice can leak information to Carol by modulating the amplitude of chirps.

Covert channel communication range. We aim to explore the effective communication range of covert channel in this experiment. Since we use AM modulation, the degree of amplitude variation influences communication range. We use *modulation depth (D)* to represent signal variations of carrier waves. We define $0 < D < 1$ as $D = M/A$, where M is the modulation amplitude (*i.e.*, peak-to-peak changes) and A is the original carrier amplitude. A larger D indicates a larger change of amplitude thus a higher SNR for covert channel. In our experiment, we observe that the communication distance between Alice and Carol is around 250 m when D=0.3. We can further increase the communication range of covert channel by increasing D. However, a larger D decreases the SNR of regular LoRa communication. We leave this for future work.

IV. Conclusion

This work investigates the vulnerability of LoRa PHY. We demonstrate the feasibility of building a covert channel by implementing `CLoRa`. `CLoRa` embeds covert information into LoRa packets by changing the amplitude of LoRa chirps while keeping the frequency intact. Experiment shows that the covert information can be decoded with high accuracy at a distance of 250 m. Our work is a pilot work which reveals the security vulnerability of LoRa PHY and LoRaWAN deployment.

Acknowledgement

This work is supported by the National Nature Science Foundation of China under grant 61702437 and Hong Kong GRF under grant PolyU 152165/19E. Yuanqing Zheng is the corresponding author.

References

[1] M. Knight and B. Seeber, "Decoding lora: Realizing a modern lpwan with sdr," in *Proceedings of the GNU Radio Conference*, vol. 1, no. 1, 2016.
[2] M. Knight. (2019) Gr-lora. https://github.com/BastilleResearch/gr-lora.
[3] Wired. (2019) Planting tiny spy chips in hardware can cost as little as $200. https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/.